下り最大 42Mbps 対応モバイル VPN ルータ

SC-RS510LS

取扱説明書

http://www.sun-denshi.co.jp/sc/

Rooster-LS

取扱説明書 目次

はじめに

表記について

本取扱説明書では、安全にお使いいただくために、守っていただきたい事項に次のマークを表示しております。

⚠警告	人体に危険を及ぼしたり、装置に大きなダメージを与えたりする可能性があることを示しています。必ずお守りください。
①注意	機能停止を招いたり、各種データを消してしまったりする可能性があることを示しています。十分に注意してください。
メモ	関連情報です。参考にお読みください。

商標について

「Rooster」「Sun Communications」は、サン電子株式会社の登録商標および商標登録出願中です。
その他、本取扱説明書に記載されている会社名、製品名は、各社の商標または登録商標です。
本文中の各社の商標または登録商標には、TM、®マークは表示しておりません。

GPL/LGPL ライセンスについて

本製品は、GPL version2.0/LGPL version2.0の適用ソフトウェアを使用しております。オープンソースとしての性格上著作権による保証はなされておりませんが、本製品につきましては保証書、および取扱説明書記載の条件により当社によ
る保証がなされています。GPL/LGPLのライセンスにつきましては、以下のURLをご覧ください。

- http://www.gnu.org/licenses/gpl-2.0.html
- http://www.gnu.org/licenses/lgpl-2.0.html

変更済みGPL対象モジュール、その配布方法につきましては、サン電子（株） サポートセンターにご連絡ください。なお、配布時発生する費用はお客様のご負担となります。

☞本取扱説明書の画面イメージは開発中のものです。
実際の画面とは多少異なる場合があります。

安全上のご注意（必ずお守りください。）

■ **ここに記載している注意事項は、安全に関わる重要な内容ですので、必ず守ってください。本取扱説明書では、安全上の注意事項を「警告」と「注意」に区分しています。**

⚠警告	この表示を無視して、間違った取り扱いをした場合、人が死亡または重傷を負う可能性が想定される内容を示しています。
⚠注意	この表示を無視して、間違った取り扱いをした場合、人が損害を負う可能性が想定される内容、および物的損害のみの発生が想定される内容を示しています。物的損害とは、家屋、家財および家畜、ペットに関する拡大損害を示しています。
	禁止行為（してはいけないこと）を示しています。
	強制行為（必ずしなければいけないこと）を示しています。

なお、注意、禁止に記載した事項でも、状況によっては重大な結果に結びつく場合があります。いずれも重要な内容を記載していますので、必ず守ってください。

⚠警告

分解禁止

本製品を分解したり、改造したりしないでください。

⇒感電、火災、故障の原因になります。

禁止

近くに雷が発生したときには AC アダプタをコンセントから抜いてご使用をお控えください。

⇒落雷が火災、感電、故障の原因となるときがあります。

禁止

本製品に水などの液体をかけたり、異物を入れたりしないでください。

⇒感電や火災の原因になります。

万一、本製品に液体がかかったり、異物が入ったりした場合は、AC アダプタをコンセントから抜いて、点検修理を依頼してください。

強制

製品から煙、異臭、異常音が発生した場合は、AC アダプタをコンセントから抜き、本製品を接続している機器からケーブルを取り外してください。また、点検修理を依頼してください。

⇒火災の原因になります。

禁止

電源ケーブルを傷つけないでください。

⇒感電、火災の原因になります。

強制

AC アダプタは、AC100V コンセントに接続してください。また、本製品を設置、移動する時は、電源プラグを抜いてください。

⇒故障、火災の原因になります。

禁止

梱包のポリ袋などは、小さいお子様の手の届く所に置かないでください。

⇒小さいお子様がかぶったり、飲みこんだりすると、呼吸を妨げる危険があります。

強制

電源プラグは確実に根元まで差し込んでください。また、電源プラグとコンセントの間のほこりは、定期的（半年に一回程度）に取り除いてください。

⇒電源プラグの間にほこりが付着し、電源が短絡して発煙、発火、火災の恐れがあります。

⚠注意

禁止

この取扱説明書に記載されている周囲環境条件以外では、使用、保管しないでください。

⇒本製品の故障や破損などによって、発煙、発火、感電の原因になります。下記の環境には、特にご注意ください。

- 室内または製品周囲の温度や湿度が極端に高い、または低い場所
- 結露がある場所
- 急激な温度変化が起きる場所
- ほこりが多い場所
- 静電気が発生しやすい場所
- 腐食性のガスが発生する場所
- 水などがかかりやすい場所
- 振動や衝撃が加わるような不安定な場所
- 油煙が当たる場所
- 直射日光が当たる場所
- 製品周囲に発熱する器具や燃えやすい物がある場所
- 周囲に置いてある物との間に適切な空間がない場所

禁止

同梱の AC アダプタ以外の電源を使用しないでください。

⇒他の電源を使用すると、故障、火災の原因になります。

強制

30cm 以上の高さから落とした場合は、使用を中止し、点検、修理を依頼してください。

⇒そのまま使用すると、重大な事故になる可能性があります。

ご使用にあたってのお願い

- **本製品周辺で静電気的障害を発生させないでください。**

  ⇒本製品は、静電気に敏感な部品を使用しています。特に、コネクタの接点、ポート、その他の部品に、素手で触れないでください。部品が静電破壊するおそれがあります。

- **本製品はていねいに取り扱ってください。**

  ⇒本製品に強いショックを与えると破損の原因になります。

- **本製品のお手入れは、電源を切った状態で行ってください。**

  ⇒誤動作や故障の原因になります。

- **本製品のお手入れには、揮発性の有機溶剤、薬品、化学ぞうきんなどを使用せず、乾いた柔らかい布で拭いてください。**
  汚れがひどい場合は、柔らかい布に台所中性洗剤をしみこませて固く絞ってから拭き、最後に乾いた柔らかい布で仕上げてください。

  ⇒揮発性の有機溶剤、薬品、化学ぞうきんなどを使用すると、変質、変色、場合によっては破損の原因になります。

地球環境保全のため、次のことにご協力ください。

- 本製品および付属品は、不燃物として処分してください。
- 廃棄方法は、地方自治体などで決められた分別収集方法に従ってください。
- 一般ごみとして、家庭で焼却処分しないでください。
  ダイオキシンや塩化水素ガスなどが発生し、環境や人体に影響を与えます。

ご注意

- **本製品の仕様は国内向けになっておりますので、海外ではご利用になれません。**

  These products are designed for use in Japan only and cannot be used in any other countries.

- **本製品は、パソコンなどの OA 機器に使用することを目的に設計、製造されています。**
  医療機器や幹線通信機器、電算機システムなどの、きわめて高い安全性や信頼性が要求される用途には使用しないでください。

- **取扱説明書について、次の点にご注意ください。**

1. 本製品は各通信事業者の USB 型データ通信端末を利用して無線によるデータ通信を行う事が出来る装置です。本製品及びモバイル通信端末等の不具合、誤動作又は停電、回線障害、その他の外部要因によって通信障害が発生した為に生じた損害等については、当社としては責任を負いかねますので、あらかじめご了承ください。
2. 本取扱説明書の内容の一部または全部を、無断で転載することを禁止します。
3. 本取扱説明書の内容に関しては、将来予告なしに変更される場合があります。
4. 本取扱説明書の内容につきましては、万全を期して作成致しましたが、万一ご不審な点や、ご不明な点、誤り、記載漏れ、乱丁、落丁、その他お気づきの点等ございましたら、当社までご連絡ください。
5. 適用した結果の影響につきましては、3 項にかかわらず責任を負いかねますので、ご了承ください。
6. 本取扱説明書で指示されている内容につきましては、必ず従ってください。本取扱説明書に記載されている内容を無視した行為や誤った操作によって生じた障害や損害につきましては、保証期間内であっても責任を負いかねますので、ご了承ください。

1. Rooster-LSの概要

1.1 主な特長

- **WiMAX や LTE、DC-HSDPA サービスに対応**

  UQコミュニケーションズWiMAX網を利用したMVNO（仮想移動体通信事業者）が提供するWiMAXサービス、およびUQコミュニケーシ ョンズのUQ WiMAXサービスやNTTドコモが提供する下り最大37.5Mbp（※1）のLTEサービス、ワイモバイルが提供する下り最大42MbpsのDC-HSDPAサービス、ソフトバンクモバイルが提供する下り最大42MbpsのHSPA＋およびDC-HSDPAに準拠した高速パケット通信サービスに対応しています。
  （※1 次世代通信LTEサービス「Xi」（クロッシィ）エリア内一部の屋内施設では受信時最大75Mbpsとなります）

- **VPN（IPsec）機能を標準搭載**

  モバイル環境によるインターネットを介した企業間のネットワークではセキュリティ確保が強く求められます。
  Rooster-LSではメインモード/アグレッシブモードの各モードに対応したハードウェア処理によるVPN（IPsec 暗号化アルゴリズム:AES256bit、3DES）機能を搭載し、モバイル通信端末を利用した高セキュリティな多拠点ネットワークを構築する事が可能です。
  またRooster-LS同士や、Rooster-G8.0ほかのRoosterシリーズとVPN接続する事も可能です。

- **サン電子が運営する商用ダイナミック DNS サービス『suncomm.DDNS』に対応**

  サン電子が運営する商用ダイナミックDNSサービス『suncomm.DDNS』に対応しています。『suncomm.DDNS』を利用する事により、固定IPアドレスを取得する事なくドメイン名（〇〇〇.suncomm.net）でインターネット上のサーバ等にアクセスする事が可能となります。

- **モバイル回線によるブロードバンド回線の冗長化を実現**

  ブロードバンド回線の障害時にHSPA等の高速なモバイル通信をバックアップ回線として利用する事を可能とするVRRP機能を搭載し、ブロードバンド回線用ルータと『Rooster-LS』を組み合わせる事でHSPA等高速なモバイル通信を利用した冗長化を可能とします。
  ※『Rooster-LS』にはブロードバンドに接続する機能は搭載しておりません。本機能を利用する場合には別途VRRP機能を搭載したブロードバンドルータが必要です。

- **長期間の安定運用を可能にする各種電源制御機能**

  高いハードウェアの耐環境性能に加え、24時間毎、曜日、時刻指定による「ソフトウェア制御によるルータの自動電源OFF/ON（モバイル通信端末が通信中は非動作、回線切断時に動作）」設定及び35時間毎又は6日毎に強制的に電源OFF/ONする「ハードウェア処理による電源OFF/ON」の機能を搭載しています。
  これらの機能を組み合わせる事で、無人環境においても長期間での安定した運用が可能になります。

- **USB2 ポート搭載により USB 型モバイル通信端末とログ保存用の USB メモリ併用が可能**

  USBポートを2ポート搭載していますので、USB型モバイル通信端末を使用しながら、USBメモリによる各種ログの保存が可能です。
  RTC及びNTPによる時刻管理された各種ログ情報が保存されます。

- **コンパクトな筐体サイズと抜け防止機構搭載**

  筐体は128×104×28mmのコンパクトなサイズを実現、設置環境の自由度が高まりました。
  またACアダプタ抜け防止クランプを同梱しておりますので、ACアダプタの抜けなどによる障害を防ぐ事が可能です。

- **高度なルータ機能を標準搭載**

  Rooster-LSは『Roosterシリーズ』で搭載されている各種ルータの基本機能を継承しています。
  NAT/IPマスカレード、ルーティング設定、DHCPサーバ/リレー、仮想サーバ、DMZ、パケットフィルタリング、NTP、ファームウェアアップデート等の各ルータ機能に加えモバイル通信端末を利用する事を前提とした、オンデマンドによる自動発信、無通信監視、WANハートビート、アドレス解決等の各種機能を搭載しています。

- **帯域制御および優先制御可能な QoS 機能を搭載**
- **安定した高度な運用を可能にする運用サポート機能を搭載**

  ・WAN ハートビート機能
  ・SNMP 機能
  ・SYSLOG 機能
  ・各種ログ機能
  ・RTC 機能

- **セッションキープ／キープアライブ機能**
- **DHCP サーバ／クライアント／リレー機能**
- **フィルタリング機能**
- **アドレス解決機能**
- **ダイナミック DNS 機能**

1.2 Rooster-LS 設定フロー

Rooster-LSを使用してダイヤルアップ接続を行う場合、最低限2までの設定を行ってください。3の設定は、必要に応じて行ってください。

1.Rooster-LS の設置

- 同梱品の確認 （☞ 1.3 同梱品の確認）
- 機器の接続 （☞ 2.1 Rooster-LS の接続方法）
- クライアント PC の設定
  （☞ 2.3 パソコンの設定（TCP/IP の設定等））

2.Rooster-LS の基本設定

- LAN、ログインパスワード、時刻、
  メールアカウントの設定
  （☞ 3.2 LAN 側の設定～
  3.5 メールアカウントの設定）
- ダイヤルアップ接続設定
  （☞ 4 ダイヤルアップ設定）

3.Rooster-LS の詳細設定（必要な場合のみ）

- RAS 着信接続設定（☞ 5.1 RAS 着信接続設定）
- WakeOn 機能設定（☞ 5.3 WakeOn 着信設定）
- 各種サービス設定（☞ 7 各種サービス設定）
- ネットワーク設定（☞ 8 ネットワーク設定）
- VPN 設定（☞ 8.7 VPN 設定）

1.3 同梱品の確認

パッケージには、次のものが同梱されています。
万一不足しているものがありましたら、お買い求めの販売店、もしくはサポートセンターにご連絡ください。

- Rooster-LS 本体　1 台
- スタートアップマニュアル（保証書付）　1 枚
- AC アダプタ　1 個
- 電源抜け防止クランプ　1 個
- ゴム足　4 個

注意　付属品にLANケーブルは含まれません。設定で使用するLANケーブルにつきましてはご利用の接続機器の速度に合わせてご用意ください。

1.4 各部の名称と機能

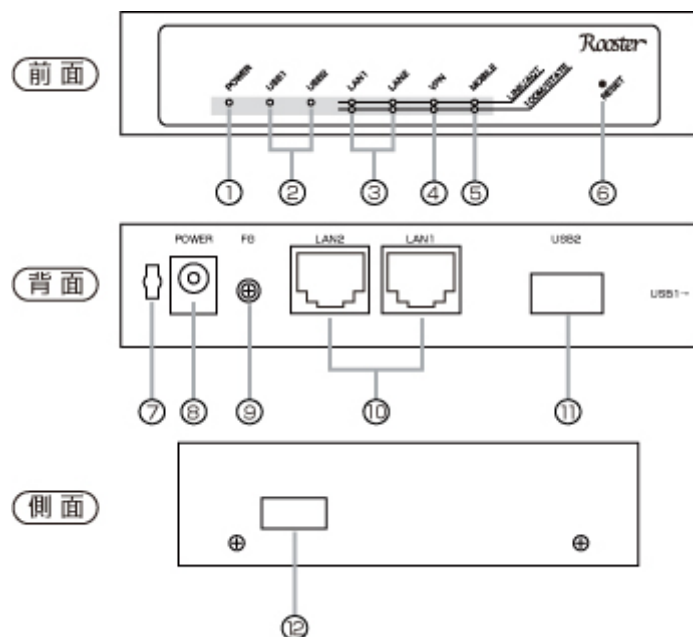



図 1–1 Rooster-LS 各部名称

- それぞれのランプの状態は、☞1.5 ランプの状態と働きをご覧ください。

1. POWER ランプ

   Rooster-LSの通電状態が表示されます。

2. USB1･2 ランプ

   USBポート(⑪･⑫)へのUSB型モバイル通信端末、またはUSBメモリの接続状態が表示されます。

3. LAN1･2 ランプ

   LANポート(⑩)へのLAN接続機器の接続状態が表示されます。

4. VPN ランプ

   VPNセッションの動作状態が表示されます。

5. MOBILE ランプ

   モバイル通信端末の動作状態が表示されます。

6. RESET スイッチ

   先の細いピンなどを使って6秒以上押し続けると、MOBILEランプ緑、橙ともに点滅し、工場出荷時の設定に戻り、再起動します。

7. クランプ取り付け穴

   電源プラグ抜け防止クランプを取り付ける穴です。

8. POWER コネクタ

   付属のACアダプタを接続します。

9. FG 端子

   アース線を接続します。

10. LAN1･2 ポート

    LANケーブルで、LAN接続機器およびハブ等を接続します。

11. USB2 ポート

    USB型モバイル通信端末またはUSBメモリを接続します。

12. USB1 ポート

    USB型モバイル通信端末またはUSBメモリを接続します。

☞電源抜け防止クランプの使い方

1. クランプを取り付けます。
2. AC アダプタを接続します。
3. クランプを閉じます。

図 1–2 電源プラグ抜け防止クランプ取り付け方法

1.5 ランプの状態と働き

- MOBILE ランプ

ランプ	状態
緑点滅	ダイヤルアップ接続で、データ通信が行われている状態です。
緑点灯	ダイヤルアップ接続が確立された状態です。
緑消灯	ダイヤルアップ接続が行われていません。
橙点灯	ダイヤルアップ接続先での認証が確立された状態です。
橙点滅	電話を掛けている状態です。
橙消灯	電話を掛けていない状態です。

- USB ランプ

ランプ	状態
緑点滅	USB メモリにログを書き込み中、または 10 秒以内に書き込みを開始します。
緑点灯	USB 型モバイル通信端末または USB メモリが認識されている状態です。
緑消灯	USB 型モバイル通信端末または USB メモリが挿入されていないか、認識されていない状態です。

USB 型モバイル通信端末や USB メモリを抜き差しする場合は Rooster-LS の電源が切れている時に行ってください。電源が入っている時は抜き差ししないでください。なお、USB ハブは使用できません。

- VPN ステータスランプ

ランプ	状態
緑点滅	VPN 接続が確立され、データ通信が行われている状態です。
緑点灯	VPN 接続が確立された状態です。
緑消灯	VPN 接続が行われていません。

- LAN1・2 ランプ

ランプ	状態
緑点滅	LAN 接続機器とのデータ通信が行われている状態です。
緑点灯	LAN 接続機器がケーブルで接続され、リンクが確立している状態です。
緑消灯	LAN 接続機器とリンクが確立してないか、ケーブルが外れています。
橙点灯	LAN 接続機器と 100Mbps で接続されている状態です。
橙消灯	LAN 接続機器 10Mbps で接続されている状態か、何も接続されていない状態です。

- POWER ランプ

ランプ	状態
緑点灯	電源が入っていて、使用可能な状態です。
緑消灯	電源が入っていません。

2. Rooster-LSの導入

2.1 Rooster-LSの接続方法

2.1.1 必要な環境

- TCP/IP が利用できる OS（Windows、MacOS、各種 UNIX など）を搭載し、イーサネットポートを搭載したパソコン
- LAN ケーブル
- Internet Explorer 8.0 以上のブラウザ
（上記以外のブラウザでは、正常に動作しない可能性があります。）

2.1.2 接続方法

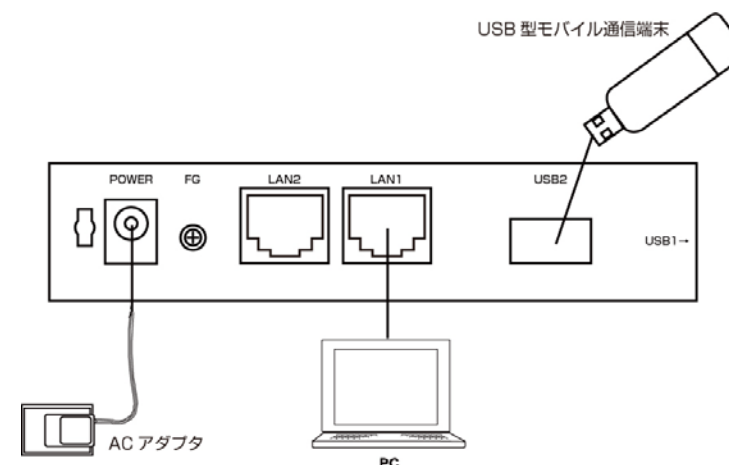



図 2-1　Rooster-LS 接続図

1. Rooster-LS とパソコンの電源が入っていないことを確認してください。
2. LAN ポートにクライアントとなるパソコンを接続してください。
3. USB 型データ通信端末、USB メモリを接続してください。
4. Rooster-LS の電源コネクタに AC アダプタを接続してください。
次に AC アダプタをコンセントに接続してください。
5. パソコンの電源を入れてください。

注意

- Rooster-LS は、モバイル通信端末専用ルータです。
  有線ブロードバンド回線に接続する機能は搭載しておりません。
- USB 型データ通信端末または USB メモリは、必ず電源を切った状態で抜き差しを行ってください。電源を入れた状態での抜き差しを行うと、Rooster-LS が作動しません。
- AC アダプタは、必ず付属のものを使用してください。
  付属以外の AC アダプタを使用すると、故障・誤作動の原因になります。
  付属以外の AC アダプタを使用された場合の故障は、保証対象外となりますのでご了承願います。
- USB メモリの種類によっては動作しないものがあります。必ず USB ランプが点灯するか、ログが正しく保存されるかを確認してください。

2.2 ご利用環境の確認

Rooster-LSとパソコンを接続するためにはパソコンにLAN環境が必要です。
LAN環境が無い場合には、ご利用のパソコンにあわせてLAN機器をご用意ください。

- パソコンで LAN ポートが標準で装備されていない場合、LAN アダプタをご利用のパソコンにあわせて増設してください。

インターネット接続の場合、通信事業者との契約が完了している必要があります。
以下についてご確認願います。

- モバイル通信端末等の回線事業者との契約、工事が完了している必要があります。
  (NTT ドコモ、ワイモバイル、等)
- インターネット接続サービスであるプロバイダとの契約が完了している必要があります。
  (OCN、@nifty 等)
  事業者によっては回線事業者とプロバイダが同じ契約の場合があります。
  その場合別途プロバイダとの契約は必要ありません。
- Rooster-LS の設定には、以下の情報が必要になります。プロバイダとの契約時に提供されている情報をご用意ください。
  不明な場合はご契約のプロバイダへお問い合わせください。
  - **アクセスポイントへの電話番号**
  - **ユーザー名**
  - **パスワード**
  - **ネームサーバ(DNS サーバ)の IP アドレス(設定が必要な場合)**

注意 アクセスポイントへの電話番号は、料金コースによって電話番号が異なりますので、お間違えのないように十分ご注意ください。

2.3 パソコンの設定(TCP/IPの設定等)

Rooster-LSにアクセスできるように、クライアントパソコンにDHCPクライアントの設定をします。
DHCPを使用しない場合は、各パソコンに手動でIPを設定する必要があります。その方法は、ネットワークカード及びWindowsのマニュアル等をご覧ください。

2.3.1 DHCPを使用する設定(Windows XPの場合)

1. コントロールパネルを開き、[ネットワークとダイヤルアップ接続]を選び、[ネットワーク接続]をダブルクリックして開きます。
   (クラシック表示の場合は、コントロールパネルを開いた後、[ネットワーク接続]のアイコンをクリックします。)

図 2-2　　ネットワーク接続

2. 「ローカルエリア接続」を右クリックし、[プロパティ]をクリックします。

ローカルエリア接続のプロパティが表示されます。

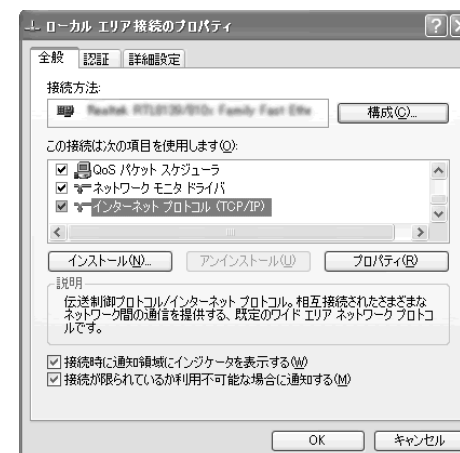



図 2-3　　ローカルエリア接続のプロパティ

3. 「インターネットプロトコル（TCP/IP）」を選び、[プロパティ]をクリックします。
   インターネットプロトコル（TCP/IP）のプロパティが表示されます。
4. 「IP アドレスを自動的に取得する」、「DNS サーバのアドレスを自動的に取得する」を選択します。

図 2-4　　インターネットプロトコル（TCP/IP）のプロパティ

5. [OK]をクリックしてダイアログを閉じます。
   [ローカルエリア接続のプロパティ]画面も、[OK]をクリックして閉じます。

2.3.2　　DHCPを使用する設定（Windows Vistaの場合）

1. パソコンには管理者権限でログインしてください。
2. 「ネットワークと共有センター」から「ネットワーク接続の管理」を開きます。

図 2-5　　ネットワークと共有センター

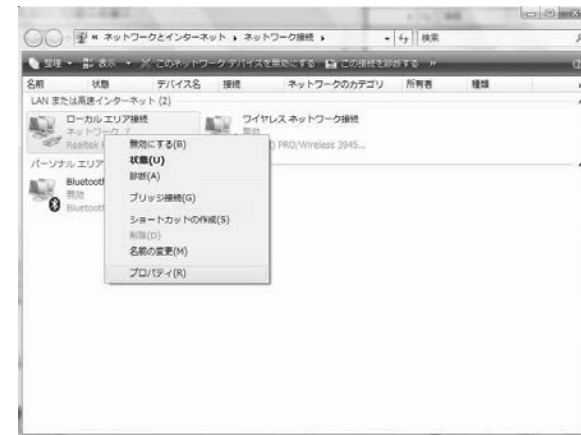



図 2-6　　ネットワーク接続の管理

3. 「ローカルエリア接続」を右クリックし、[プロパティ]をクリックします。
   ローカルエリア接続のプロパティが表示されます。

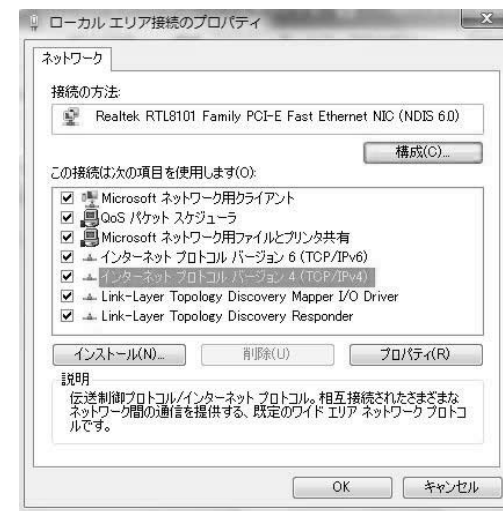



図 2-7　　ローカルエリア接続のプロパティ

4. 「インターネットプロトコル　バージョン 4（TCP/IPv4）」を選び、[プロパティ]をクリックします。
   インターネットプロトコルバージョン 4（TCP/IPv4）のプロパティが表示されます。
5. 「IP アドレスを自動的に取得する」、「DNS サーバのアドレスを自動的に取得する」を選択します。

図 2-8　インターネットプロトコル　バージョン 4（TCP/IPv4）のプロパティ

6. [OK]をクリックしてダイアログを閉じます。
   [ローカルエリア接続のプロパティ]画面も、[OK]をクリックして閉じます。

2.3.3　DHCPを使用する設定（Windows 7の場合）

1. パソコンには管理者権限でログインしてください。
2. コントロールパネルから「ネットワークとインターネット」を開きます。

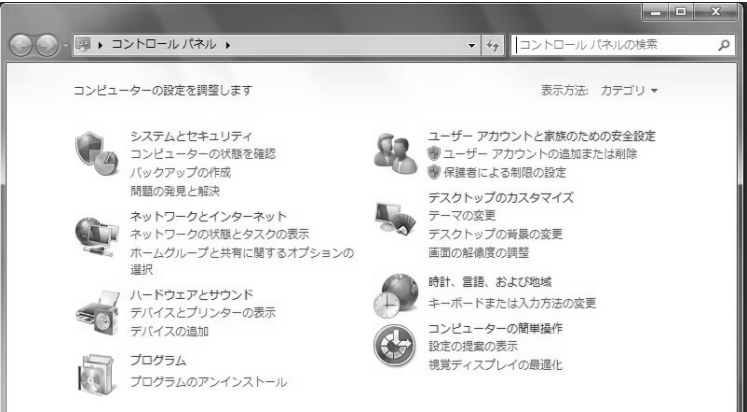



図 2-9　コントロールパネル

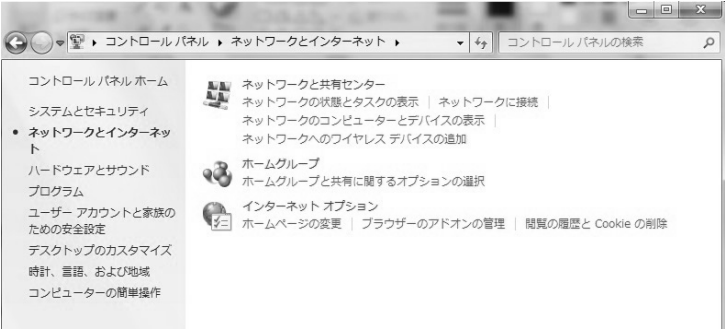



図 2-10　ネットワークとインターネット

3. 「ネットワークと共有センター」を開きます。

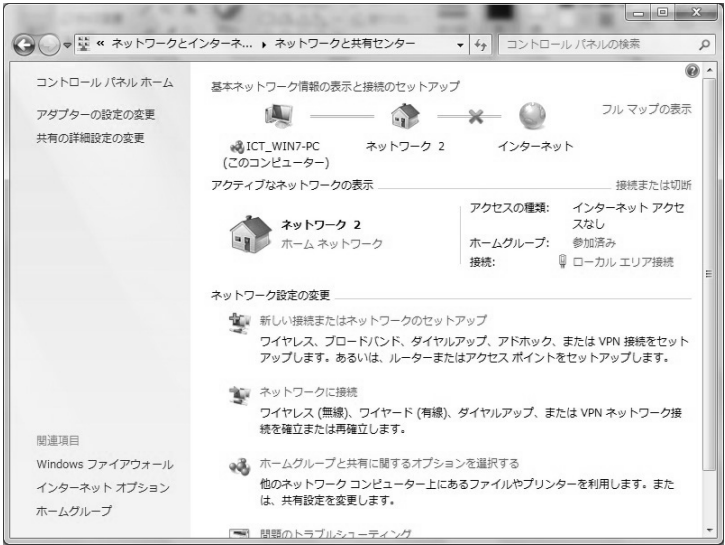



図 2-11　ネットワークと共有センター

4. 「アダプターの設定の変更」を開きます。

図 2-12　アダプターの設定の変更

5. 「ローカルエリア接続」を右クリックし、[プロパティ]をクリックします。
   ローカルエリア接続のプロパティが表示されます。

図 2-13　アダプターの設定の変更

6. 「インターネットプロトコル　バージョン 4（TCP/IPv4）」を選び、[プロパティ]をクリックします。
   インターネットプロトコルバージョン 4（TCP/IPv4）のプロパティが表示されます。
7. 「IP アドレスを自動的に取得する」、「DNS サーバのアドレスを自動的に取得する」を選択します。

図 2-14　インターネットプロトコル　バージョン 4（TCP/IPv4）のプロパティ

8. [OK]をクリックしてダイアログを閉じます。
   [ローカルエリア接続のプロパティ]画面も、[OK]をクリックして閉じます。

3. Rooster-LSの初期設定

3.1 Rooster Web設定ツールへのログイン方法

9. WWW ブラウザを起動します。
10. WWW ブラウザのアドレス入力欄に、Rooster-LS の LAN 側 IP アドレス「http://192.168.62.1/」（工場出荷時状態）を入力し、Enter を押します。

図 3-1　Rooster-LS IP アドレスの入力

ログインダイアログボックスが表示されます。

図 3-2　ネットワークパスワードの入力画面

11. ユーザー名に「admin」、パスワードに「1234」(工場出荷時状態)と入力した後、OK ボタンをクリックします。
12. Rooster-LS の設定ツールが表示されます。

注意

- 設定ツールは JavaScript を使用しています。
  ブラウザの JavaScript をオンにしてから設定を行ってください。
- 設定ツールを表示し、しばらく放置すると、一旦ログアウト処理を行います。その後、設定ツールにアクセスすると、再度ログインダイアログボックスが表示されます。
- ここで入力するユーザー名、パスワードは、Rooster-LS の設定ツールにアクセスするためのもので、プロバイダから提供されるユーザー名、パスワードとは異なるものです。
  （パスワードの変更方法は、☞3.3 ログインパスワードの設定をご覧ください。）

Rooster 設定

本体設定

インターフェイス

各種サービス

ネットワーク

ログ

ステータス

図 3-3　　Rooster-LS Web 設定ツール

3.2　LAN側の設定

Rooster-LSのLAN側IPアドレスを変更する場合に設定を行います。
工場出荷時状態のLAN側IPアドレスは「192.168.62.1」に設定されています。

1. 設定ツールのメニューから、[インターフェイス]－[LAN]をクリックします。

「LAN側設定」のページが表示されます。

インターフェイス

インターフェイスの各設定を行います。

LAN

LAN側の各設定を行います。

IPアドレス: 192.168.62.1

サブネットマスク: 255.255.255.0

RIP 機能を使用する。

設定

図 3-4　　LAN 側設定画面

2. [IP アドレス]、[サブネットマスク]に、新しく設定する Rooster-LS の LAN 側 IP アドレス、サブネットマスクを入力します。
3. RIP によるダイナミックルーティングに対応させる場合、「RIP 機能を使用する」のチェックをオンにします。
4. [設定] ボタンをクリックして、設定を反映させます。

注意 IP アドレス変更後は、一旦ブラウザを閉じてしばらくお待ちください。その後、新しく設定した IP アドレスで再度設定ツールにログインします。

なお、変更前と異なるサブネットの IP アドレスに変更した場合、
（例.192.168.62.1⇒192.168.0.1 に変更）
Rooster-LS、パソコン共に再起動を行ってください。

LAN内の通信状態は、設定ツールのメニューから、[ステータス]－[LAN]をクリックして表示される「LANステータス表示画面」から確認することができます。

ステータス

現在の設定・状態を表示します。

LAN

LAN内の通信状態を表示します。

MACアドレス:		
IPアドレス:		192.168.62.1
サブネットマスク:		255.255.255.0
ステータス	LAN1:	接続中
	LAN2:	未接続
送信バイト数:		312676 バイト
送信パケット数:		582 パケット
送信エラー回数:		0 回
受信バイト数:		158453 バイト
受信パケット数:		1276 パケット
受信エラー回数:		0 回

図 3-5　　LAN ステータス表示画面

■　**MAC アドレス**

Rooster-LSのMACアドレスが表示されます。

■　**IP アドレス**

Rooster-LSのIPアドレスが表示されます。

■　**サブネットマスク**

Rooster-LSのサブネットマスクが表示されます。

■ **ステータス（LAN1･2）**

LANポート1･2へのLAN接続機器の接続状態が表示されます。

■ **送信バイト数**

Rooster-LSから送信したデータの総バイト数が表示されます。

■ **送信パケット数**

Rooster-LSから送信したデータの総パケット数が表示されます。

■ **送信エラー回数**

Rooster-LSからデータ送信を行った際に発生したエラー回数の総計が表示されます。

■ **受信バイト数**

Rooster-LSで受信したデータの総バイト数が表示されます。

■ **受信パケット数**

Rooster-LSで受信したデータの総パケット数が表示されます。

■ **受信エラー回数**

Rooster-LSがデータ受信を行った際に発生したエラー回数の総計が表示されます。

3.3 ログインパスワードの設定

ログインパスワードを変更する場合に設定を行います。
工場出荷時状態のパスワードは｢1234｣に設定されています。

1. 設定ツールのメニューから、[本体設定]－[パスワード変更]をクリックします。
   「パスワードの変更」ページが表示されます。

本体設定
本体の各設定を行います。
パスワード変更
ログインパスワードの変更を行います。
古いパスワード:
新しいパスワード:
再入力:
変更

図 3-6　　パスワード変更画面

2. [古いパスワード]に、現在使用しているパスワードを入力します。
3. [新しいパスワード]に、新しく設定するパスワードを入力します。
4. [再入力]に、[新しいパスワード]に入力したパスワードを再度入力します。
5. 設定 ボタンをクリックして、設定を反映させます。
6. ログインダイアログボックスが表示されます。新しく設定したパスワードで再度ログインします。

注意
- 入力したパスワードはすべて、｢＊｣で表示されます。
- 入力可能な文字数は、半角英数字、記号で 16 文字までです。
- ユーザー名の変更はできません。“admin”のみとなります。

3.4 時刻の設定

ここで設定される時刻は、Rooster-LS のログ表示などに使用されます。
（ログ表示の詳細は、☞ 9 ログの参照方法をご覧ください。）

設定ツールのメニューから、[本体設定]－[時刻設定] をクリックします。
｢時刻設定｣ページが表示されます。

図 3-7　　時刻設定画面

3.4.1 NTPサーバを使用して定期的に時刻を同期する場合

注意 この機能を使用するには、インターネットに接続している必要があります。（☞インターネット接続設定の詳細は、4.3 ダイヤルアップ接続設定をご覧ください。）

1. 「NTP サーバ機能を使用する。」チェックをオンにし、以下の設定を行います。

■ **NTP サーバ名 1**

時刻を問合せるNTPサーバアドレス1を入力します。

■ **NTP サーバ名 2**

時刻を問合せるNTPサーバアドレス2を入力します。

■ **問合せ間隔**

指定された間隔でサーバにNTPサーバに接続し、時刻を同期します。
“0”を設定した場合、Rooster-LSの起動後、1回のみ同期します。

2. [設定] ボタンをクリックして、設定を反映させます。

設定完了後、[今すぐ問合せを行う] ボタンをクリックすると、設定したNTPサーバに接続して時刻を同期します。

注意 NTP 問合せに失敗した場合は、成功するまで約 5 分間隔で問合せを実行します。

3.4.2 手動で時刻の設定を行う場合

1. [手動設定]の各欄に、現在の時刻を入力します。
2. [手動設定] ボタンをクリックします。直ちに設定した時刻に調整されます。

注意 時刻同期を行う際、WAN 回線が接続されていない場合、モバイル通信端末の設定（☞4.3 ダイヤルアップ接続設定をご覧ください。）によっては自動的にダイヤルを行います。

3.5 メールアカウントの設定

メモ ここで設定されるメールアカウントは、Rooster-LS の、メール送信によるアドレス解決機能（機能の詳細は、☞ 7.1 アドレス解決機能をご覧ください。）に使用されます。

メール送信によるアドレス解決機能を使用する必要がない場合、メールアカウントの設定の必要はありません。

1. 設定ツールのメニューから、[本体設定]－[メールアカウント設定] をクリックします。

「メールアカウントの設定」ページが表示されます。

図 3-8 メールアカウント設定画面

2. 以下の設定を行います。

■ **サービスの種類**

メールサーバの種類を選択します。
「POP Before SMTP」、「ユーザ認証 SMTP」のいずれかを選んでください。

■ **SMTP サーバ名**

送信メールサーバ名を設定します。

■ **SMTP ポート番号**

送信ポート番号を設定します。

■ **POP3 サーバ名**

受信メールサーバ名を設定します。

■ **アカウント**

アカウント名を設定します。

■ **パスワード**

使用するメールアカウントのパスワードを入力します。

注意 上記の設定で不明な部分につきましては、インターネットプロバイダ、あるいはサーバ管理者までお問い合わせください。

3. [設定] ボタンをクリックして、設定を反映させます。

3.6 電源制御

Rooster-LSの電源の制御を行います。この機能は定期的にRooster-LSの電源を OFF/ON することにより、より安定した運用を行うことを目的とします。

1. 設定ツールのメニューから、[本体設定]－[電源制御] をクリックします。

「電源制御」のページが表示されます。

本体設定

本体の各設定を行います。

電源制御

自動電源ON/OFFの設定を行います。

☑ ハードウェアの自動電源ON/OFF機能を使用する。

◉ 35時間毎　○ 6日毎

☑ ソフトウェアの自動電源ON/OFF機能を使用する。

動作条件： ○ 回線接続中は電源ON/OFFしない。

◉ 回線接続中でも電源ON/OFFする。

○ 間隔指定

間隔： 1日

◉ 時刻指定

03 時 00 分 (00:00～23:59)

○ 毎日

◉ 曜日指定

☑：月 ☐：火 ☑：水 ☐：木

☑：金 ☐：土 ☑：日

設定

図 3-9　　電源制御設定画面

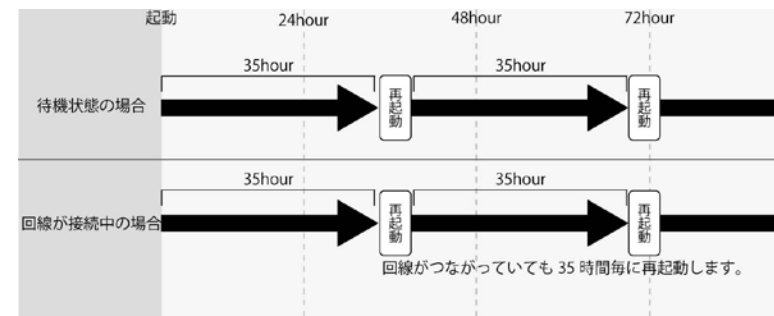
2. 以下の設定を行います。

■ **ハードウェア**

ハードウェア上でRooster-LSの電源をOFF/ONするための設定です。
使用する場合はチェックを入れ、「35時間毎」、「6日毎」のいずれかを選択します。

メモ　ソフトウェアの設定が何らかの影響にて動作しなかった時の保険的な機能です。

注意
- 回線がつながっている状態でも、設定時間になるとハードウェアが再起動します。
- ハードウェアの設定時間は目安ですので、実際の動作時間は多少前後します。

<例>
ハードウェア：35時間毎

■ **ソフトウェア**

ソフトウェア上でRooster-LSの電源をOFF/ONするための設定です。
使用する場合はチェックを入れ、以下の設定を行ってください。

- 動作条件

回線接続中の際に電源をON/OFFするか否かを選択します。

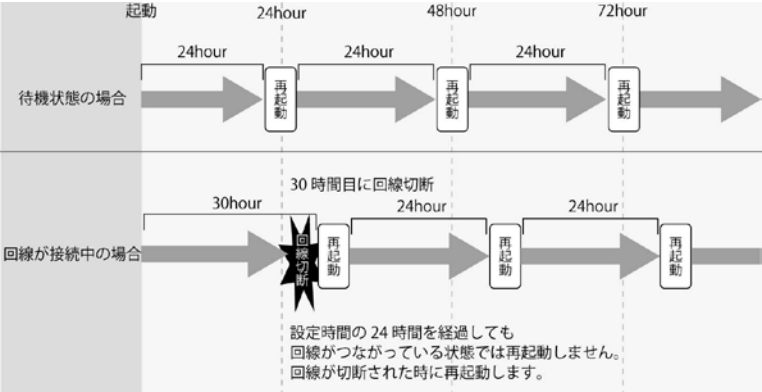
注意　“回線接続中でも電源 ON/OFF する”を選択した場合、設定時間がきたら通信を行っている場合でも強制的に再起動をします。

- 間隔指定

ソフトウェアにおいて、日にち間隔で設定する場合はチェックを入れ間隔を1～7日の間で設定します。

- 時刻指定

再起動させたい時刻を指定します。24時間表記にて設定します。またその曜日を「毎日」または「曜日指定」にて設定します。

<例>
ソフトウェア:使用する、回線接続中は電源OFF/ONしない、1日毎

3. 選択した設定でよければ ボタンをクリックします。
4. 設定を反映させるためには、Rooster-LS を再起動させる必要があります。

> ※メモ　モバイル通信端末については、24 時間毎にリセットする機能が搭載されています。回線がつながっている状態ではモバイル通信端末は再起動せず、回線切断後に再起動します。

4. ダイヤルアップ設定

4.1 プロバイダ情報の確認

インターネット接続の設定を行う場合は、以下のインターネットサービスプロバイダ（以下プロバイダ）等から提供された情報を用意してください。
☞ 2.2 ご利用環境の確認をご覧ください。

- **アクセスポイントへの電話番号**
  （料金コースによって電話番号が異なりますので、お間違えのないように十分ご注意ください。）
- **ユーザー名**
- **パスワード**

4.2 APN設定機能

> ※メモ　Rooster-LS では、モバイル通信端末の APN 設定の確認や書込み、Rooster への APN 設定が可能です。新しく APN の設定を追加する場合は、ご契約のインターネットサービスプロバイダ（以下プロバイダ）等からご提供された情報をご用意ください。
>
> ・APN（アクセスポイントネーム） ・ユーザ名 ・パスワード
>
> モバイル通信端末にデフォルトで登録されている APN を利用する場合はこの機能の利用は必要ありません。
>
> ※APN の設定機能は、ファームウェアバージョン 4.00 以降の機能です。

1. 設定ツールのメニューから、[インターフェイス]－[モバイル通信端末]をクリックします。
「モバイル通信端末」のページが表示されます。

インターフェイス

インターフェイスの各設定を行います。

モバイル通信端末

モバイル通信端末の設定を行います。

☑ APN設定機能を使用する。

APNの設定

モード	使用	操作
ダイヤルアップ	使用しない	設定
RAS着信	使用しない	設定
WakeOn着信	使用しない	設定

初期化ATコマンド:

設定

図 4-1　　APN 設定機能画面

2. APN 設定機能を利用する場合は、「APN 設定機能を使用する」のチェックをオンにし [設定] ボタンをクリックして設定内容を反映させます。

「APN の設定」を行う前に、ここで一度、[設定] ボタンをクリックして、設定内容を反映させます。
「APN の設定」を先にクリックすると、設定した内容が破棄されてしまいます。

4.2.1 APN設定

1. 「APN の設定」をクリックします。「APN の設定」のページが表示されます。

インターフェイス

インターフェイスの各設定を行います。

モバイル通信端末：APN設定

APNの設定を行います。

RoosterのAPN設定を使用する。 [設定]

APNを追加する。 [追加]

CID	APN	プロトコル	メモ	操作
1	abc.suncomm.ne.jp	PPP	suncomm	変更 削除

[戻る]

図 4-2　APN 設定画面

2. どの APN 設定を使用するかを以下のいずれかより選択します。

- ■ モバイル通信端末の APN 設定を使用する
- ■ Rooster の APN 設定を使用する。

※メモ

【モバイル通信端末の APN 設定を使用する】場合

モバイル通信端末内の APN 設定を Rooster に読み出し、モバイル通信端末へ設定します。

[設定] ボタンをクリックすると、挿入されているモバイル通信端末に登録されている APN を読み込み、表示します。

【Rooster の APN 設定を使用する】場合

Rooster 内の APN 設定をモバイル通信端末へ設定します。

工場出荷時、Rooster には APN は設定されていません。必ず [追加] ボタンをクリックし、APN 設定を行ってください。

3. [設定] ボタンをクリックして設定内容を反映させます。

注意

【モバイル通信端末の APN 設定を使用する】を選択時、再起動後に、モバイル通信端末に登録されている APN を読み込み、WEB 設定画面へ表示されます。

なお、モバイル通信端末のステータスが、「待受中」または「使用しない」の場合のみ、モバイル通信端末の APN を表示・設定が可能です。

【Rooster の APN 設定を使用する】を選択時、Rooster に APN が設定されていない場合はモバイル通信端末に登録されている APN を全て消去しますのでご注意ください。予めモバイル通信端末に登録されている APN を控えておくことを推奨します。
モバイル通信端末のステータスが「待受中」または「使用しない」タイミングでモバイル通信端末へ APN を設定します。

4. 新しく APN の登録を行う場合は、[追加] ボタンをクリックします。設定済みの APN を変更する場合は、[変更]をクリックします。
5. [追加] ボタン、または[変更]をクリックすると、「APN 設定の詳細設定」ページが表示されます。
[追加] ボタンをクリックした場合は空白の状態で、[変更]をクリックした場合は、「APN 設定の詳細設定」ページが表示され、表示されている APN 設定の変更が行えます。
[削除]をクリックすると、表示されている接続先設定が削除されます。
[戻る] ボタンをクリックすると、「モバイル通信端末設定」のページに戻ります。

注意

- ● 設定可能な APN 設定の件数はモバイル通信端末で異なります。
- ● 追加登録時、CID 項目に登録済の cid 番号を入力して登録すると、登録済の cid 番号へ APN 設定が上書きされます。

APN設定の詳細設定

CID	1
APN	abc.suncomm.ne.jp
プロトコル	PPP
メモ	suncomm

[設定] [キャンセル]

図 4-3　APN 設定画面

6. 以下の設定を行います。

■ **CID**

登録するcid番号を入力します。

> **注意** APN 設定の変更時は入力できません。

■ **APN**

ご契約のプロバイダのアクセスポイントネームを入力します。

■ **プロトコル**

プロトコルタイプを選択します。
「IP」または「PPP」のいずれかを選択します。

■ **メモ**

設定内容を分かりやすくするための覚え書きを入力します。
半角16文字（全角8文字）までの任意の文字列を入力できます。

> **注意** **【モバイル通信端末の APN 設定を使用する】場合**は入力できません。

7. [設定] ボタンをクリックして設定内容を反映させます。
   [キャンセル] ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「APN の設定」のページに戻ります。

4.3 ダイヤルアップ接続設定

1. 設定ツールのメニューから、[インターフェイス]－[モバイル通信端末]－[ダイヤルアップ]をクリックします。

「ダイヤルアップ接続設定」のページが表示されます。

インターフェイス
インターフェイスの各設定を行います。
モバイル通信端末：ダイヤルアップ
モバイル通信端末の設定（ダイヤルアップ接続）を行います。
必要な場合は「RAS着信」および「フィルタリング」の設定を行ってください。
☑ ダイヤルアップ接続を行う。
ダイヤルアップ先の設定
ダイヤルアップモード： 通常
☑ 自動接続を行う。
☐ セッションキープを行う。
☑ LCP Echo Requestによる接続監視を行う。
10 秒間隔
5 回連続無応答で切断
☑ 無通信監視を行う。 600 秒
☑ NATを使用する。
本体側IPアドレス： ◉ 自動取得 ○ IP固定
IPアドレス：
認証プロトコル： 相手に合わせる
暗号化： 無効
設定

図 4-4　　ダイヤルアップ接続設定画面

2. 「ダイヤルアップ接続を行う。」のチェックをオンにし、以下の設定を行います。

> **注意** 必要な場合は「RAS 着信」（☞ 5.1 RAS 着信接続設定）および「フィルタリング」（☞ 8.3 FORWARD フィルタリング、8.4 INPUT フィルタリング）の設定を行ってください。

■ **ダイヤルアップ先の設定**

クリックすると、モバイル通信端末によるダイヤルアップ接続先の表示、追加が行えます。（設定方法は、☞ 4.3.1 ダイヤルアップ接続先の追加、変更方法をご覧ください。）

■ ダイヤルアップモードの設定

ダイヤルアップのモードを選択します。
「通常」、「対向通信」、「ビジネスmopera」、「unnumbered」、「WiMAX」のいずれかを選択します。

> **注意** ご利用のモバイル通信端末によっては、ご利用いただけないモードがあります。対応するモバイル通信端末は、弊社ホームページの対応機種一覧をご覧ください。
> http://www.sun-denshi.co.jp/sc/ls/card.html

● モードが「通常」、「WiMAX」の場合

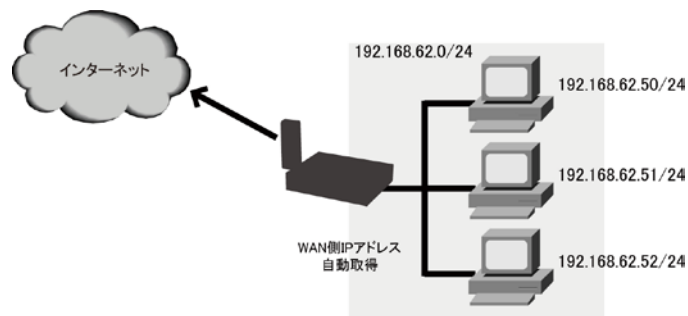



図 4-5　モード「通常」での接続例

インターネットへ接続される場合には「通常」を選択ください。
WAN側のIPアドレスが固定の場合には「本体側IPアドレス」に、指定のIPアドレスを入力してください。

> **注意** モードが「WiMAX」の場合、必ず Rooster の「時刻設定」(☞ 3.4 時刻の設定)を行ってください。
> WiMAX 端末と Rooster を接続する場合は、必ず USB 延長ケーブルを使用してください。動作確認された USB 延長ケーブルは弊社ホームページをご覧ください。
> http://www.sun-denshi.co.jp/sc/ls/card.html

> **メモ** モード「WiMAX」の設定は、ファームウェアバージョン：Version4.01 から実装された項目です。

● モードが「対向通信」の場合

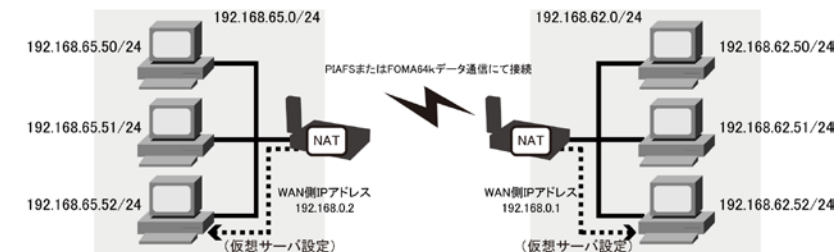



図 4-6　モード「対向通信」で「NAT 使用する」場合の接続例

NATを使用する場合は、仮想サーバもしくはDMZの設定が必要となります。
設定につきましては☞ 8.5 バーチャルサーバまたは☞ 8.6 DMZをご覧ください。

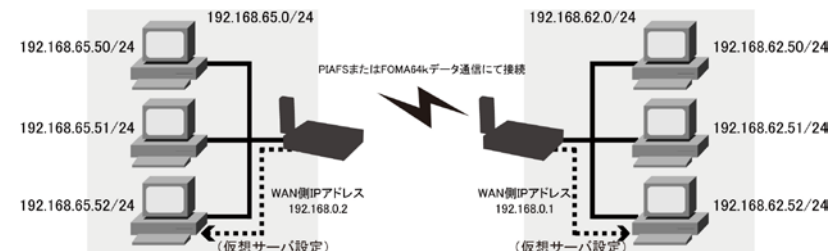



図 4-7　モード「対向通信」で「NAT 使用しない」場合の接続例

NATを使用しない場合は、お互いのLAN側のIPアドレスでの通信が可能になります。

● モードが「ビジネス mopera」の場合

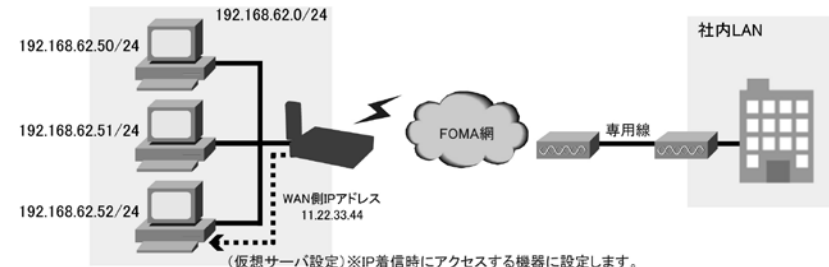



図 4-8　モード「ビジネス mopera」での接続例

NTTドコモのビジネスmoperaアクセスプレミアム/アクセスプロをご利用の際には、「ビジネスmopera」を選択ください。

注意 NTT ドコモとの契約が必要になります。
ビジネス mopera アクセスプレミアム/アクセスプロにつきましては、NTTドコモのホームページをご覧ください。

- モードが「Unnumbered」の場合

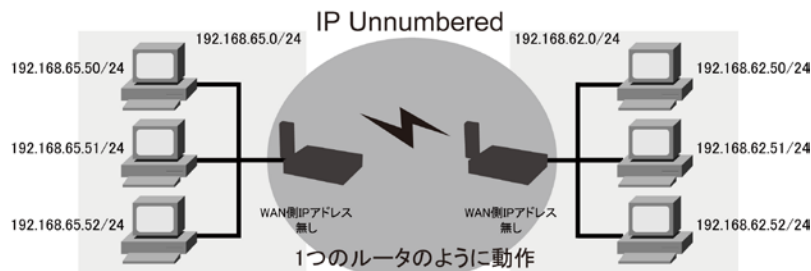



図 4-9　モード「Unnumbered」での接続例

Unnumbered接続とは、他のネットワークに接続するルータのWAN側にIPアドレスを割り当てず、2台のルータを見かけ上1台のルータのように扱う接続方式です。このようにWAN側にIPアドレスを付与せず接続する場合には「Unnumbered」を選択ください。

■ **自動接続を行う**

チェックをオンにすると、LAN側から発信要求があった場合、もしくはRooster-LSの各種サービスによる接続要求があった場合等に、自動発信が行われるようになります。
セッションキープの設定は、自動接続の設定をオンにするとできるようになります。
チェックをオフにすると、接続、切断の動作は設定ツールのみで行うようになります。

■ **セッションキープを行う**

回線接続を維持させておきたい時にチェックをオンにします。

注意 従量制課金でご契約の場合は、設定しないようにしてください。
意図しない接続で通信料金が掛かってしまう原因となりますので、くれぐれもご注意願います。

■ **LCP Echo Request による接続監視を行う**

チェックをオンにすると、LCP Echo Requestを送信します。
送信間隔、切断動作をさせる回数を設定します。

LCP Echo Request による接続監視はファームウェアバージョン:6.00 から実装されたものです。

■ **無通信監視を行う**

チェックをオンにすると、Rooster-LSに指定した秒数の間、通信が行われなかった時、自動的に回線を切断するようになります。
チェックがオンになっていても、“0”を入力した場合、無通信監視は行いません。

注意 従量制課金でご契約の場合は、必ず設定するようにしてください。

■ **NAT を使用する**

WAN側への通信を行う際にIPアドレスの変換が必要になる場合、チェックをオンにします。
インターネット接続を行う場合、通常はチェックをオンにしてください。

■ **本体側 IP アドレス:自動取得**

WAN側のIPアドレスが自動取得の場合はこちらを選択します。

■ **本体側 IP アドレス:IP 固定**

WAN側のIPアドレスが固定の場合はこちらを選択します。

■ **IP アドレス**

本体側IPアドレスを「IP固定」で選択した際には、IPアドレスを入力します。

注意 「ダイヤルアップモード」の設定で、「対向通信」を選択した場合は、IP アドレスを Rooster-LS の LAN 側 IP とは別のネットワーク IP アドレスを指定ください。また IP アドレスは「RAS 着信接続」で設定したクライアント IP アドレスと合わせてください。設定方法につきましては☞ 5.1 RAS 着信接続設定をご覧ください。

■ **認証プロトコル**

ダイヤルアップの認証プロトコルを選択します。
「CHAP」、「PAP」、「相手に合わせる」、「MS-CHAPv2」のいずれかを選択します。
「MS-CHAPv2」を選択した場合、暗号化の設定が有効になります。

メモ 認証プロトコルの設定項目「CHAP」「PAP」は、ファームウェアバージョン:Version5.00 から実装された項目です。

■ **暗号化**

暗号化の設定を選択します。
「無効」または「MPPE128bit」のどちらかを選択します。

3. ［設定］ボタンをクリックして、設定内容を反映させます。

注意 「ダイヤルアップ先の設定」を行う前に、ここで一度、［設定］ボタンをクリックして、設定内容を反映させます。
「ダイヤルアップ先の設定」を先にクリックすると、設定した内容が破棄されてしまいます。

4.3.1 ダイヤルアップ接続先の追加、変更方法

1. 「ダイヤルアップ先の設定」をクリックします。
   「ダイヤルアップ接続先リスト」のページが表示されます。

インターフェイス

インターフェイスの各設定を行います。

モバイル通信端末：ダイヤルアップ

ダイヤルアップ接続先リストの設定を行います。

No.	電話番号	ID	接続方式	メモ	操作
1	*99***1#	suncomm	通常ダイヤルアップ	memo	変更 削除

戻る

図 4-10　ダイヤルアップ接続先リスト画面

2. 新しく接続先の登録を行う場合は、追加 ボタンをクリックします。設定済みのダイヤルアップ接続先を変更する場合は、[変更]をクリックします。
   戻る ボタンをクリックすると、「ダイヤルアップ接続設定」のページに戻ります。
3. 追加 ボタン、または[変更]をクリックすると、「ダイヤルアップ接続先の詳細設定」ページが表示されます。
   追加 ボタンをクリックした場合は空白の状態で、[変更]をクリックした場合は、「ダイヤルアップ接続先の詳細設定」ページが表示され、表示されている接続先設定の変更が行えます。
   [削除]をクリックすると、表示されている接続先設定が削除されます。
   戻る ボタンをクリックすると、「ダイヤルアップ接続設定画面」のページに戻ります。

注意 設定可能な接続先は 1 件のみです。

ダイヤルアップ接続先の詳細設定

No.	1
電話番号	*99***1#
ID	suncomm
パスワード	●●●●●●●
接続方式	通常ダイヤルアップ
メモ	memo

設定　キャンセル

図 4-11　ダイヤルアップ接続先設定画面

4. 以下の設定を行います。

■ **電話番号**

アクセスポイントへの電話番号を入力します。
電話番号の-(ハイフン)は、入力してもしなくても構いません。
電話番号設定の詳細は、☞ 4.5.1 インターネット接続の料金コースと専用通信方式をご覧ください。

注意 アクセスポイントへの電話番号は、料金コースによって電話番号が異なりますので、お間違えのないように十分ご注意ください。

■ **ID**

プロバイダから提供されたユーザ名を入力します。

■ **パスワード**

プロバイダから提供されたパスワードを入力します。

● 上記の設定でご不明な部分につきましては、インターネットサービスプロバイダ、あるいはサーバ管理者までお問い合わせください。

■ **接続方式**

「通常ダイヤルアップ」のみの設定となります。

■ **メモ**

設定内容を分かりやすくするための覚え書きを入力します。
半角16文字（全角8文字）までの任意の文字列を入力できます。

5. 設定 ボタンをクリックして設定内容を反映させます。
   キャンセル ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「ダイヤルアップ接続先リスト」のページに戻ります。

4.4 接続/切断方法

1. 設定ツールのメニューから、[ステータス]－[モバイル通信端末] をクリックします。
「モバイル通信端末ステータス」のページが表示されます。

ステータス

現在の設定・状態を表示します。

モバイル通信端末

モバイル通信端末での通信状態を表示します。

No.	ステータス	接続先	操作
1	ダイヤルアップ接続完了 詳細表示	*99***1# suncomm	切断 無効

図 4-12　モバイル通信端末ステータス表示画面(接続完了状態)

■ **ステータス（ダイヤルアップ接続時）**

設定したダイヤルアップ接続の現在の状態が表示されます。
[詳細表示]をクリックすると、現在の状態をより詳しく参照できます。

表 4-1　モバイル通信端末のステータス一覧

ステータス表示	状態	本体 Mobile ランプの状態	
		緑	橙
無効	接続設定が無効になっています。	消灯	消灯
未装備	モバイル通信端末が挿入されていないか、モバイル通信端末が認識できていません。	消灯	消灯
使用しない	モバイル通信端末は正常に認識されていますが、接続設定が行われていません。	消灯	消灯
未動作	モバイル通信端末制御サービスが一時停止しています。モバイル通信端末の再起動を行っている時などに表示されます。	消灯	消灯
待受中	モバイル通信端末が正常に認識されていて、接続設定も行われていますが、接続が行われていない状態です。	消灯	消灯
ダイヤルアップ発信中	接続先へ電話を掛け始めた状態です。	消灯	点滅
ダイヤルアップ PPP ネゴ中	プロバイダ（RAS サーバ）で認証を行っている状態です。	点灯	点滅
ダイヤルアップ接続完了	接続が正常に行えた状態です。	点灯	点灯

注意 電源を入れた状態でモバイル通信端末の抜き差しを行うと、モバイル通信端末が挿入されていても、ステータスが “未装備” となる場合があります。この場合、Rooster-LS の再起動を行ってください。
またモバイル通信端末の抜き差しは、必ず電源を切った状態で行ってください。

■ **接続先**

設定した接続先電話番号が表示されます。

■ **操作**

それぞれ以下の操作を行います。

- [接続]⇒接続動作を行います。
- [切断]⇒切断動作を行います。
- [無効]⇒設定を無効にします。
  次回、[有効]をクリックするまで設定内容を使えないようにします。
- [有効]⇒設定を有効にします。
  次回、[無効]になっている設定を再度使えるようにします。

4.4.1 通信ステータス詳細表示

モバイル通信端末通信の詳細表示

No.	1
ステータス:	ダイヤルアップ接続完了
電話番号:	*99***1#
ユーザ名:	suncomm
IPアドレス:	[illegible]
ゲートウェイ:	[illegible]
DNSサーバ1:	[illegible]
DNSサーバ2:	[illegible]

送信バイト数:	97 バイト
送信パケット数:	5 パケット
送信エラー回数:	0 回
受信バイト数:	64 バイト
受信パケット数:	4 パケット
受信エラー回数:	0 回

戻る

図 4-13 モバイル通信端末ステータス詳細表示画面

■ **ステータス**

設定したダイヤルアップ接続の現在の状態が表示されます。

■ **電話番号**

設定したアクセスポイントへの電話番号が表示されます。

■ **ユーザー名**

設定したユーザー名が表示されます。

■ **IP アドレス**

プロバイダおよび接続先から割り当てられた、Rooster-LSのWAN側IPアドレスが表示されます。

■ **ゲートウェイ**

ゲートウェイのIPアドレスが表示されます。

■ **DNS サーバ 1**

DNSサーバ1のIPアドレスが表示されます。

■ **DNS サーバ 2**

DNSサーバ2のIPアドレスが表示されます。

■ **送信バイト数**

モバイル通信端末で送信したデータの総バイト数が表示されます。

■ **送信パケット数**

モバイル通信端末で送信したデータの総パケット数が表示されます。

■ **送信エラー回数**

モバイル通信端末でデータ送信を行った際に発生した、エラー回数の総計が表示されます。

■ **受信バイト数**

モバイル通信端末で受信したデータの総バイト数が表示されます。

■ **受信パケット数**

モバイル通信端末で受信したデータの総パケット数が表示されます。

■ **受信エラー回数**

モバイル通信端末でデータ受信を行った際に発生した、エラー回数の総計が表示されます。

ダイヤルアップ接続が正常に行えない場合、本体ランプの点灯状況、およびステータス、ログなどから、その原因の切り分けを行うことができます。

ステータス、本体ランプの点灯状況は、☞ 4.4 接続/切断方法を、ログ表示の詳細は、☞ 9 ログの参照方法をご覧ください。

4.5 対応通信モード一覧

4.5.1 インターネット接続の料金コースと専用通信方式

通信業者	ご利用の料金コース	通信方式の名称	電話番号の形式
（株）ウィルコム	つなぎ放題 [8×]、[4×]	PRO/8×/4x パケット方式	〈電話番号〉##64
	つなぎ放題 [1×]	1x パケット方式	〈電話番号〉##61
	ネット 25 [8×]、[4×]	PRO/8×/4x パケット方式	〈電話番号〉##64
	ネット 25	フレックス チェンジ方式	〈電話番号〉##7
	3G	パケット通信	＊99#
	XGP	パケット通信	＊99##92
（株）エヌ・ティ・ティ・ドコモ	FOMA	7.2M パケット通信	注 1) ＊99＊＊＊●#
		64k 回線交換	＊9601
	LTE	37.5M パケット通信	注 3） APN 指定
イー・モバイル（株）	EM モバイル ブロードバンド	7.2M パケット通信	＊99＊＊＊1#
		42M・21M パケット通信	注 2） APN 指定
（株）インターネットイニシアティブ	IIJ モバイル	7.2M パケット通信	＊99＊＊＊1#
		21M パケット通信	注 2） APN 指定
KDDI（株）	CDMA 1X WIN	3.6M パケット通信	＊99＊＊24#
	LTE	75Mbps パケット通信	＊99＊＊＊1#
ソフトバンクモバイル（株）	アクセスインターネット	42M・7.2M パケット通信	＊99＊＊＊1#
		3.6M パケット通信	＊99#
		64k 回線交換	＊7300
UQ コミュニケーションズ（株）	WiMAX	40M パケット通信	なし

注1)●は、APNの設定で登録を行ったcid番号（1-10）が入ります。
（moperaでは初期値は ”1” 、moperaUでは初期値は ”3”となります。）
mopera以外の登録を行う場合は、FOMAの取扱説明書等をご覧ください。
NTTドコモの定額プランをご利用のお客様は下記URLをご参照ください。
http://www.teigaku-docomo.net/manualsetting/index.html
IIJ mobileも＊99＊＊＊●＃にて設定ください。APNの設定につきましてはモバイル通信端末の取扱説明書をご覧ください。

注2）プロバイダがイー・モバイルの場合、電話番号はemb.ne.jpまたはemb2.ne.jpです。
プロバイダがIIJモバイルの場合、電話番号はiijmobile.jpです。

注3）プロバイダがmoperaUの場合、電話番号はmopera.netです。

注意

- イー･モバイルのデータ通信端末利用で、「データプラン B」をご契約の場合、プランのプロトコル制限から、VPN 接続が出来ません。また、「データプラン B」における網側の仕様上、外部からのアクセスが出来ませんのでご注意ください。
  例）WEB カメラを接続して、外部からアクセスしたい場合、データプラン B ではご利用いただけません。
- イー・モバイルのデータ通信端末において、PC 接続ツールで最後に接続された APN が cid 番号の 1 番に適用されます。PC 接続ツールでデータプラン B に接続したのち、Rooster-LS で「＊99＊＊＊1#」へダイヤルをおこなった場合、データプラン B へ接続されますのでご注意ください。
- WiMAX 端末を使用する場合、使用中は Rooster-LS 本体を移動しないでください。
- WiMAX 端末を使用する場合、事前に PC でのサインアップを行ってください。
- KDDI の USB STICK LTE をご利用の場合、あらかじめ端末をモデムモードに切り替えていただく必要がございます。切り替えツールにつきましては KDDI へお問い合わせください。また、LTE エリア外でご利用された場合は、CDMA 1X の接続となりますので予めご了承ください。

注意

- 電話番号の設定は、必ず接続先、通信方式をご確認の上、正しく設定を行うようにしてください。
  定額制でのご契約でも、専用の接続先、通信方式以外で通信を行った場合、基本料金とは別に通信料金が発生します。
- パケット通信方式は、パケット通信で接続可能なプロバイダの場合のみ使用できます。
  それ以外の場合は、回線交換方式で接続を行います。
- パソコンにモバイル通信端末のドライバをインストールする必要はありません。Rooster-LS が自動認識します。
  ただし、モバイル通信端末に付属のユーティリティソフトは、Rooster-LS 経由では動作致しません。
- モバイル通信端末のサービスエリア外（圏外）では使用できません。（モバイル通信端末の表示ランプを確認してください。）
- モバイル通信端末のサービスエリア内でも、電波の受信状況が悪い場合、回線が混んでいる場合などには、通信が不安定になることもあります。

5. 着信設定

5.1 RAS着信接続設定

メモ

RAS 着信機能について

RAS（Remote Access Service）とは、電話回線を通じて遠隔地のネットワークにダイヤルアップ接続し、そのネットワークの資源を利用する機能をいいます。

注意

ご利用のモバイル通信端末によっては、ご利用いただけないモードがあります。対応するモバイル通信端末は、弊社ホームページの対応機種一覧をご覧ください。
http://www.sun-denshi.co.jp/sc/ls/card.html

1. 設定ツールのメニューから、[インターフェイス]－[モバイル通信端末]－[RAS 着信] をクリックします。

「RAS着信」設定のページが表示されます。

図 5-1　RAS 着信設定画面

2.「RAS 着信接続を行う。」チェックをオンにし、以下の設定を行います。

> **注意** 必要な場合は「ダイヤルアップ接続」(☞ 4.3 ダイヤルアップ接続設定)および「フィルタリング」(☞8.3 FORWARD フィルタリング、8.4 INPUT フィルタリング)の設定を行ってください。

■ **RAS 着信モード**

RAS着信モードを選択します。
「通常」、「対向通信」、「ビジネスmopera」、「Unnumbered」のいずれかを選択します。

● モードが「通常」の場合

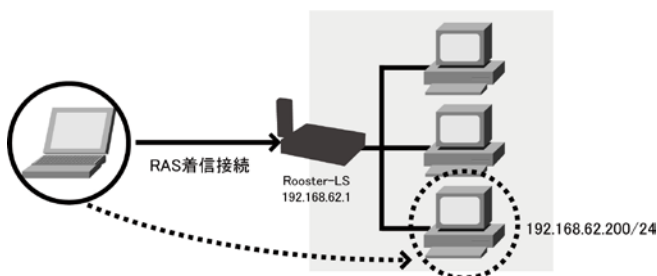



図 5-2 モードが「通常」の場合の接続

外部からアクセスしたパソコンのIPアドレスはRooster-LSのLAN側のIPアドレスとなります。

● モードが「対向通信」の場合

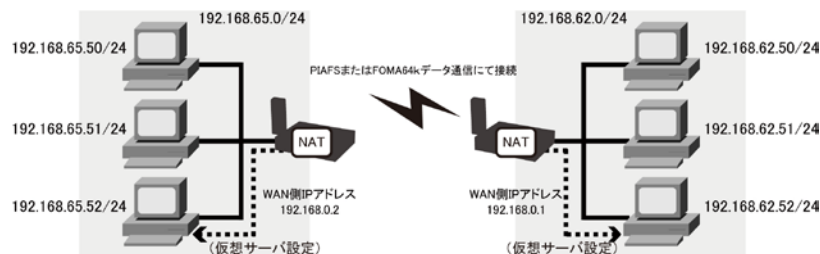



図 5-3 モード「対向通信」で「NAT 使用する」場合の接続例

NATを使用する場合は、仮想サーバもしくはDMZの設定が必要となります。
設定につきましては☞ 8.5 バーチャルサーバまたは☞ 8.6 DMZをご覧ください。

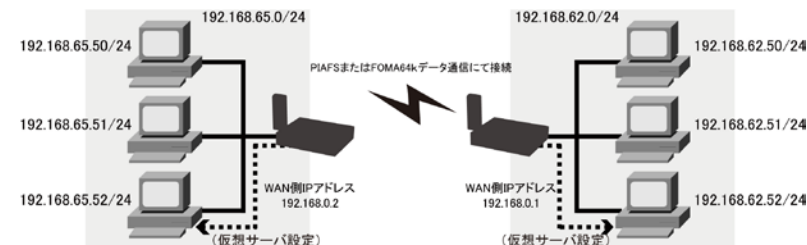



図 5-4 モード「対向通信」で「NAT 使用しない」場合の接続例

NATを使用しない場合は、お互いのLAN側のIPアドレスでの通信が可能になります。

● モードが「ビジネス mopera」の場合

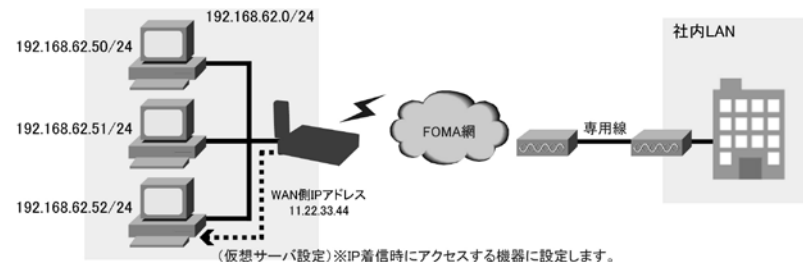



図 5-5 モード「ビジネス mopera」での接続例

NTTドコモのビジネスmoperaアクセスプレミアムのIP着信オプションをご利用の際には、「ビジネスmopera」を選択ください。

> **注意** NTT ドコモとの契約が必要になります。
>
> ビジネス mopera アクセスプレミアムにつきましては、NTT ドコモのホームページをご覧ください。

● モードが「Unnumbered」の場合

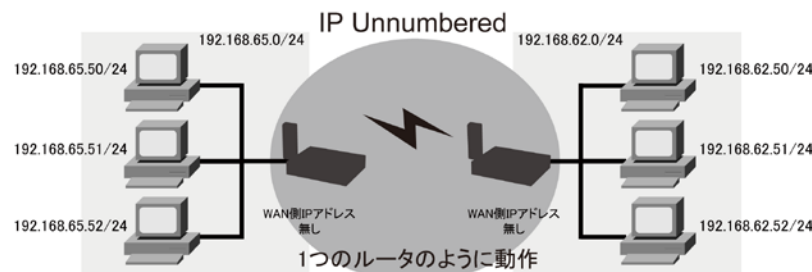



図 5-6 モード「Unnumbered」での接続例

Unnumbered接続とは、他のネットワークに接続するルータのWAN側にIPアドレスを割り当てず、2台のルータを見かけ上1台のルータのように扱う接続方式です。このようにWAN側にIPアドレスを付与せず接続する場合には「Unnumbered」を選択ください。

■ **着番認証を行う**

相手先の電話番号でも認証を行いたい場合、チェックをオンにします。
オンにすると、「着番リストの設定」へのリンク(☞ 5.1.1着信番号での認証設定をご覧ください。) が有効となります。

■ **認証プロトコル**

認証の際に使用するプロトコルを選択します。
「CHAP」、「PAP」、「相手に合わせる」、「MS-CHAPv2」のいずれかを設定します。
「MS-CHAPv2」を選択した場合、暗号化の設定が有効になります。

> ①注意 RAS 着信モードを「通常」で選択した場合、認証プロトコルは「CHAP」または「PAP」でのみ接続が可能となります。

■ **暗号化**

暗号化の設定を選択します。
「無効」または「MPPE128bit」のどちらかを選択します。

■ **クライアントの IP アドレス**

RAS着信でログインを行ったクライアントに割り当てるIPアドレスを設定します。

> ①注意 クライアントの IP アドレスの設定について
>
> 「RAS 着信モード」で「通常」を選択した場合は以下の条件を満たすものを設定してください。
>
> - Rooster-LS の LAN IP アドレスと同じネットワーク内の IP アドレス。
> - DHCP サーバ機能をオンにしている場合、その割り当てられる範囲以外の IP アドレス。
>
> 「RAS 着信モード」で「対向通信」を選択した場合は以下の条件を満たす IP アドレスを設定してください。
>
> - LAN 側のネットワークとは別のネットワーク IP アドレスを設定してください。
> - 「ダイヤルアップ接続」の設定で、「本体側の IP アドレス」で設定した IP アドレスと同じネットワークアドレスを設定してください。

■ **本体側 IP アドレス:自動取得**

WAN側のIPアドレスが自動取得の場合はこちらを選択します。

■ **本体側 IP アドレス:IP 固定**

「RAS着信モード」で「対向通信」または「ビジネスmopera」を選択した場合、本体側のIPアドレスを固定にて設定する場合に選択ください。

■ **IP アドレス**

本体側IPアドレスを「IP固定」で選択した際には、IPアドレスを入力します。

> ①注意 「RAS 着信モード」で「対向通信」を選択した場合には、「クライアント IP アドレス」で設定した IP アドレスと同じネットワークアドレスを入力ください。
>
> 例:クライアント IP アドレス:192.168.100.1
> 　本体側 IP アドレス:192.168.100.2

■ **ユーザー設定**

認証に使用するユーザー名、パスワードを入力します。

■ **NAT を使用する**

「RAS着信モード」で「通常」以外を選択した場合、必要に応じて設定してください。

3. [設定] ボタンをクリックします。

> ①注意 引き続いて「着信番号での認証設定」も行う場合は、ここで一度、[設定] ボタンをクリックして、設定内容を反映させます。
> **先にクリックすると、設定した内容が破棄されてしまいます。**

5.1.1 着信番号での認証設定

Rooster-LSでは、ユーザ名、パスワードによる認証と同時に、発信者電話番号による認証を行うことも可能です。

1. 「着番リストの設定」をクリックします。

「RAS着信相手先リスト」のページが表示されます。

インターフェイス

インターフェイスの各設定を行います。

モバイル通信端末:RAS着信

RAS着信リストの設定を行います。

着信受け入れ先を追加する。 [追加]

No.	電話番号	メモ	操作
1	09012345678	RAS	変更 削除

[戻る]

図 5-7　　RAS 着信相手先リスト画面

2. RAS 着信相手先の追加を行いたい場合は、追加 ボタンをクリックします。RAS 着信相手先を変更する場合は、[変更]をクリックします。
(戻る ボタンをクリックすると、「RAS 着信」設定のページに戻ります。)

メモ 着信相手先の設定は最大 50 件まで行えます。

「RAS着信相手先の詳細設定」ページが表示されます。

RAS着信リストの詳細設定

No.	01
電話番号	09012345678
メモ	RAS

設定 キャンセル

図 5-8 RAS 着信相手先設定画面

3. 以下の設定を行います。

■ 電話番号

RAS着信相手先の電話番号を入力します。
電話番号の-(ハイフン)は、入力してもしなくても構いません。

■ メモ

設定内容を分かりやすくするための覚え書きを入力します。16文字までの任意の文字列を入力できます。

4. 設定 ボタンをクリックし、設定内容を反映させます。
キャンセル ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「RAS 着信リスト」のページに戻ります。

5.1.2 RAS着信時のステータス表示

1. 設定ツールのメニューから[ステータス]－[モバイル通信端末]をクリックします。
「モバイル通信端末ステータス」のページが表示されます。

ステータス

現在の設定・状態を表示します。

モバイル通信端末

■ モバイル通信端末での通信状態を表示します。

No.	ステータス	接続先	操作
1	着信接続完了 詳細表示	test	切断 無効

図 5-9 モバイル通信端末ステータス表示画面(着信接続完了状態)

■ **ステータス(RAS 着信時)**

設定したRAS着信の現在の状態が表示されます。
[詳細表示]をクリックすると、現在の状態をより詳しく参照できます。

表 5-1 モバイル通信端末のステータス一覧

ステータス表示	状態	本体 Mobile ランプの状態	
		緑	橙
無効	接続設定が無効になっています。	消灯	消灯
未装備	モバイル通信端末が挿入されていないか、認識できていません。	消灯	消灯
使用しない	モバイル通信端末は正常に認識されていますが、接続設定が行われていません。	消灯	消灯
待受中	モバイル通信端末が正常に認識されていて、接続設定も行われていますが、接続が行われていない状態です。	消灯	消灯
着信接続中	遠隔地からの接続機器のアクセスを確認した状態です。	消灯	点滅
着信 PPP ネゴ中	Rooster-LS で、接続機器の認証を行っている状態です。	点灯	点滅
着信接続完了	着信接続が正常に行えた状態です。	点灯	点灯

注意 電源を入れた状態でモバイル通信端末の抜き差しを行うと、モバイル通信端末が挿入されていても、ステータスが "未装備" となる場合があります。この場合、Rooster-LS の再起動を行ってください。
またモバイル通信端末の抜き差しは、必ず電源を切った状態で行ってください。

注意
- RAS 着信はモバイル通信端末ログに記録されます。
（ログ表示の詳細は、☞9.2.1 モバイル通信端末ログをご覧ください。）

5.2 ダイヤルアップ接続設定とRAS着信設定の併用

Rooster-LSでは、ダイヤルアップ接続設定とRAS着信を併用させることが可能です。
待受中に着信があった場合は、RAS着信の設定が有効になり、着信動作を行います。
逆に待受中に接続要求があった場合は、ダイヤルアップ接続の設定が有効となり、ダイヤルアップ動作を行います。

- ダイヤルアップ接続設定は、☞ 4 ダイヤルアップ設定をご覧ください。
- RAS 着信接続設定は、☞ 5.1 RAS 着信接続設定をご覧ください。

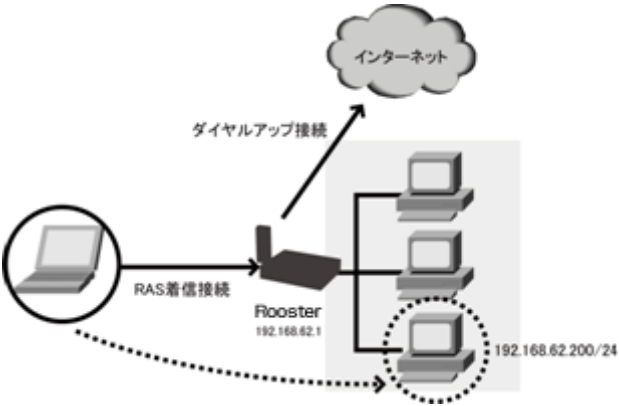



図 5-10　ダイヤルアップ接続と RAS 着信接続

注意
- RAS 着信接続とダイヤルアップ接続は排他使用となります。
(同時にお使いいただくことはできません。)
- ダイヤルアップ接続の各設定と RAS 接続の各設定は独立していますので、それぞれ設定してください。

5.3 WakeOn着信設定

メモ　WakeOn 着信について

待ち受け状態のモバイル通信端末を、遠隔地からの操作によりダイヤルアップさせることを可能とする機能です。

KDDI（株）のセンタープッシュサービスに対応しています。

また AIR-EDGE 端末によるライトメール、および携帯電話等からによる音声着信、FOMA での TV 電話着信にも対応しています。

注意 ご利用のモバイル通信端末によっては、ご利用いただけない場合があります。対応するモバイル通信端末は、弊社ホームページの対応機種一覧をご覧ください。
http://www.sun-denshi.co.jp/sc/ls/card.html

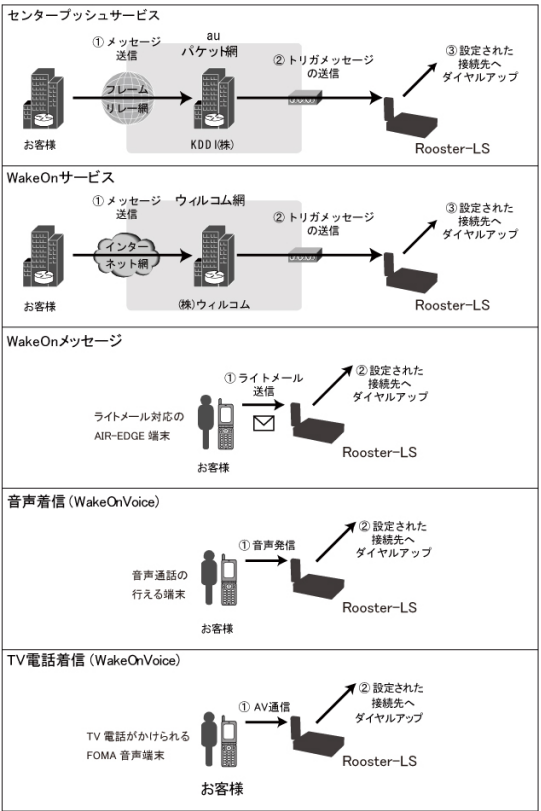



図 5-11　WakeOn 着信機能の概要

1. 設定ツールのメニューから、[インターフェイス]－[モバイル通信端末]－[WakeOn 着信]をクリックします。

「モバイル通信端末：WakeOn着信」設定のページが表示されます。

インターフェイス
インターフェイスの各設定を行います。
モバイル通信端末：WakeOn着信
モバイル通信端末の設定（WakeOn着信）を行います。
☑ WakeOn着信を行う。
メッセージの種類：◉ WakeOnメッセージを受け付ける。（ライトメール／WakeOnサービス／センタープッシュサービス）
○ FOMA TV電話着信、音声着信を受け付ける。(WakeOn Voice機能)
認証キー：1234（無記入はチェック無し）
☑ 着番認証を行う。 着番リストの設定
設定

図 5-12　WakeOn 着信設定画面

2. 「WakeOn 着信を行う。」チェックをオンにし、以下の設定を行います。

■ **WakeOn メッセージを受け付ける。**

WakeOnメッセージを受信してWakeOn着信を行う場合は、こちらを選択します。

■ **FOMA TV 電話着信、音声着信を受け付ける。(WakeOn Voice 機能)**

FOMAのTV電話着信、または音声着信を受信してWakeOn着信を行う場合は、こちらを選択します。

■ **認証キー**

WakeOnメッセージの文字列による認証を行えます。
「WakeOnメッセージを受け付ける。」設定を有効にした時に設定できます。
認証キーは、（受信したメッセージの先頭文字）～（設定された認証キー文字数）までを比較し、一致した場合は成功となります。
ただし、一文字でも異なった場合は認証失敗となります。
なお空白の場合、認証は行いません。認証キーは半角英数字のみです。

表 5-2　WakeOn メッセージ認証設定例

設定した認証キー	受信したメッセージ	結果	
1234	5678	×	全く一致していないため
1234	1234	○	全文字一致しているため
12	1234	○	先頭 2 文字が一致しているため
12345	1234	×	5 文字目が一致しないため

■ **着番認証を行う**

WakeOnを行う発信端末を限定させたい場合、チェックをオンにすると、発信者電話番号で認証を行うことができます。
オンにすると「着番リストの設定」へのリンクが有効となります。

3. [設定] ボタンをクリックして、設定内容を反映させます。

注意 引き続いて「着番リストの設定」も行う場合は、ここで一度、[設定]ボタンをクリックして、設定内容を反映させます。
先にクリックすると、設定した内容が破棄されてしまいます。

5.3.1　着信番号での認証設定

1. 「着番リストの設定」をクリックします。

「WakeOn着信相手先リスト」のページが表示されます。

インターフェイス
インターフェイスの各設定を行います。
モバイル通信端末：WakeOn着信
WakeOn着信リストの設定を行います。
着信受け入れ先を追加する。 追加

No.	電話番号	メモ	操作
1	09012345678	WakeOn	変更 削除

戻る

図 5-13　WakeOn 着信リスト画面

2. WakeOn 着信リストの追加を行いたい場合は、[追加] ボタンをクリックします。設定済みの WakeOn 着信相手先を変更する場合は、[変更]をクリックします。
[戻る] ボタンをクリックすると、「WakeOn 着信設定画面」のページに戻ります。

[追加] ボタンまたは、[変更]をクリックすると、「WakeOn着信リストの詳細設定」ページが表示されます。
[追加] ボタンをクリックした場合は空白の状態で、[変更]をクリックした場合は、設定済みの情報が入力された状態で開きます。
[削除]をクリックすると、表示されているWakeOn着信リスト設定が削除されます。

メモ 着信相手先の設定は最大 16 件まで行えます。

図 5-14　WakeOn 着信リスト設定画面

3. 以下の設定を行います。

■ **電話番号**

WakeOn着信相手先の電話番号を入力します。
電話番号の－（ハイフン）は、入力してもしなくても構いません。

■ **メモ**

設定内容を分かりやすくするための覚え書きを入力します。半角16文字 (全角8文字)までの任意の文字列を入力できます。

4. 設定 ボタンをクリックし、設定内容を反映させます。
キャンセル ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「WakeOn 着信相手先リスト」のページに戻ります。

注意
- センタープッシュのサービスを利用する場合は、KDDI（株）との契約が必要です。

注意
- WakeOn 着信による発信は、モバイル通信端末ログに記録されます。（ログ表示の詳細は、☞9.2.1 モバイル通信端末ログをご覧ください。）
- 音声着信(WakeOn Voice)の場合、電話を掛ける端末は、発信者番号通知、および音声発信が行える端末で可能ですが、Rooster-LS 側で使用可能なモバイル通信端末は、対応する一部のモバイル通信端末のみとなります。対応するモバイル通信端末は、弊社ホームページの対応機種一覧をご覧ください。
http://www.sun-denshi.co.jp/sc/ls/card.html

6. Rooster-LS メンテナンス

6.1 設定情報の保存、読み込み

設定ツールのメニューから、[本体設定]－[設定情報の保存、読み込み] をクリックします。
「設定情報の保存、読み込み」のページが表示されます。

本体設定

本体の各設定を行います。

図 6-1　設定情報保存、読み込み画面

6.1.1 現在の設定を保存

[現在の設定]テキストボックス内の設定情報の保存を行います。

1. [設定の保存]の 保存 ボタンをクリックします。
「rooster.cfg」がダウンロードされます。

図 6-2　コンフィグファイルのダウンロード（Windows XP SP2 の場合）

2. 保存(S) ボタンをクリックし、「rooster.cfg」の保存先を指定します。
Rooster-LSの設定情報が、指定した保存先にダウンロードされます。

6.1.2　保存した設定の読み込み

1. [設定の読み込み]の 参照 ボタンをクリックし、読み込みを行う設定情報ファイル「*.cfg」のある場所を指定します。
2. 読み込み開始 ボタンをクリックします。

Rooster-LSの設定が保存時の設定に書き戻されます。

> **注意** ファームウェアのアップデートにおいて、違ったメジャーバージョンのファームウェアの設定情報ファイルは読み込めません。
>
> 詳細につきましては☞6.3 ファームウェアのアップデート方法をご覧ください。

6.2 設定情報の消去

1. 設定ツールのメニューから、[本体設定]－[設定の消去] をクリックします。

「設定の消去」のページが表示されます。

本体設定

本体の各設定を行います。

設定の消去

設定情報を消去して出荷時の状態に戻します。

工場出荷時の設定に戻す 消去

図 6-3　　設定情報消去画面

2. [工場出荷時の設定に戻す]の 消去 ボタンをクリックします。

確認ダイアログで[OK]をクリックすると、Rooster-LSが再起動し、設定が工場出荷時の状態にリセットされます。

> **注意** 設定情報の初期化は、Rooster-LS 本体にあるリセットスイッチの長押しでも行うことができます。
>
> その方法は、☞1.4 各部の名称と機能をご覧ください。

6.3 ファームウェアのアップデート方法

> **メモ** アップデートファイルは、新しいモバイル通信端末への対応、機能追加、プログラム修正などが行われるたびに、弊社ホームページにて随時公開を行う予定です。
>
> 下記の手順を行う前に、以下のページよりファームウェアのイメージファイルをダウンロードしてください。
>
> **Rooster-LS 製品情報**
>
> http://www.sun-denshi.co.jp/sc/ls/

> **注意** **【現状ファームウェアバージョン 2.00 以前の場合】**
>
> ファームウェアのアップデートにおいて、違うメジャーバージョンへアップデートする場合、設定情報が全て工場出荷時に初期化されます。
>
> WEB 設定画面における「設定情報の保存・読み込み」も出来ませんのでご了承ください。
>
> - **ファームウェアのバージョン情報の見方**
>
>
>
>
> 現状のファームウェアのバージョンをご確認いただき、アップデートするファームウェアのメジャーバージョンが違う場合は、設定情報が引き継げません。（工場出荷時に初期化されます）
>
> マイナーバージョン番号のみの場合は、設定情報は引き継がれます。
>
> **【現状ファームウェアバージョン 3.00 以降の場合】**
>
> 設定情報は引き継がれます。
>
> 但し、バージョンダウンを行った場合、設定情報は引き継がれず、全て工場出荷時に初期化されますのでご注意ください。

1. 設定ツールのメニューから、[本体設定]－[ファームウェアアップデート] をクリックします。「ファームウェアのアップデート」ページが表示されます。

本体設定

本体の各設定を行います。

ファームウェアアップデート

ファームウェアのアップデートを行います。

現在のファームウェアバージョン:
RS510LS-6.00, Aug 16 2013 16:54:20

アップデート開始ボタンを押すと、指定されたファームウェアに書き換えを行います。
ファイル名: 参照... アップデート開始

図 6-4　　ファームウェアアップデート画面

2. 参照 ボタンをクリックして、ダウンロードしたアップデートプログラムデータ「*.img」のある場所を指定します。
3. アップデート開始 ボタンをクリックします。

確認ダイアログで[OK]をクリックすると、Rooster-LSのファームウェアがアップデートされます。

注意
- アップデートを実行すると、SNMP 機能を使用している場合強制停止されます。SNMP 機能の詳細につきましては、☞ 7.7 SNMP をご覧ください。
- ファームウェアのマイナーバージョンアップデートは、メジャーバージョン番号が一致している必要があります。また、マイナーバージョンのアップデートは、新しいバージョンへのアップデートのみ可能です。（古いバージョンへ戻すことが出来ません）
- メジャーバージョン変更のファームウェアのイメージファイルは約 10M バイトあります。従量課金のご契約でのダウンロードにはご注意ください。

警告
ファームウェアのメジャーバージョンアップデートでは完了するまで、10 分程度かかります。**アップデート中は、背面の AC アダプタを絶対に抜かないようにしてください。動作不能となる恐れがあります。**

これにより動作不能となった場合、有償修理となりますのでご注意願います。

6.4 Rooster-LSの再起動

1. 設定ツールのメニューから、[本体設定]－[再起動] をクリックします。

「再起動」ページが表示されます。

本体設定

本体の各設定を行います。

再起動

本体を再起動させます。

再起動ボタンを押すと、本体が再起動します。 再起動

図 6-5　　再起動画面

2. 再起動 ボタンをクリックします。

注意 再起動が完了するまで、2 分程度かかります。

7. 各種サービス設定

7.1 アドレス解決機能

※メモ　アドレス解決機能について

外部ネットワークから、インターネットに接続された Rooster-LS にアクセスする場合、Rooster-LS に割り当てられたグローバル IP アドレスの情報が必要になりますが、通常のインターネット接続ではインターネットに接続するたびに、グローバル IP アドレスは任意に変化します。

Rooster-LS では、変化するグローバル IP アドレスを指定メールアカウントに通知する機能、ダイナミック DNS サーバを利用する機能のいずれかの方法によって、上記問題を解決することができます。

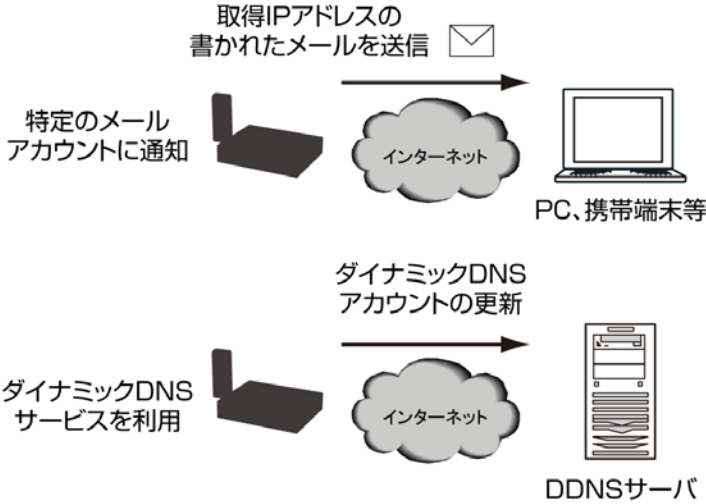



図 7-1　　アドレス解決機能の概要

各種サービス

各種サービスの設定を行います。

アドレス解決

アドレス解決の設定を行います。

☑ アドレス解決機能を使用する。

更新時間の間隔: 5 分 (0の場合、自動更新)

◯ 特定のメールアカウントに通知する。

メールアカウントの設定

送信先メールアドレス:

送信元メールアドレス:

メール送信の設定:

◉ 標準のメッセージを送信する。　◯ 指定のメッセージを送信する。

指定のメッセージ:

(IPアドレスは、'%s'と表記してください。)

◉ ダイナミックDNSサービスを利用する。

サービスの種類: suncomm.DDNS

サーバ名: www.suncomm.jp

ホスト名: rooster.suncomm.net

アカウント: suncomm

パスワード: •••••••

設定

図 7-2　　アドレス解決機能設定画面

設定ツールのメニューから、[各種サービス]－[アドレス解決]をクリックします。「アドレス解決」設定のページが表示されます。
アドレス解決機能を使用する場合は、「アドレス解決機能を使用する。」チェックをオンにし、以下の設定を行います。

7.1.1　　IPアドレスを指定メールアカウントに通知する設定

1. 「特定のメールアカウントに通知する。」のチェックをオンにし、以下の設定を行います。

■ **更新時間の間隔**

指定メールアカウントに、設定された時間ごとにメール送信します。“0”を設定した場合自動更新となり、グローバルIPアドレスが変更された時のみ、メール送信を行います。
“0”以外を設定される場合、設定の最小値は5（分）となります。

■ **メールアカウントの設定**

（設定方法は☞ 3.5 メールアカウントの設定をご覧ください。）

> **注意** 引き続いて「メールアカウントの設定」も行う場合は、ここで一度 設定 ボタンをクリックして、設定内容を反映させます。
> 設定 ボタンよりも先に「メールアカウント設定」をクリックすると、設定した内容が破棄されます。

■ **送信先メールアドレス**

グローバルIPアドレスを通知させたいメールアドレスを入力します。

> **メモ** 送信先メールアドレスを複数設定したい場合は、“，”区切りで設定いただけます。
>
> 設定可能文字数は区切りの“，”を含めて 63 文字までです。

■ **送信元メールアドレス**

送信者のメールアドレスを入力します。

> **注意** 送信元メールアドレスの入力がないと、メールサーバによってはメールが送信されない場合があります。

■ **メール送信の設定**

通知メールのメッセージ内容を指定したい場合は、「指定のメッセージを送信する。」を選択します。必要がなければ、「標準のメッセージを送信する。」を選択します。
標準のメッセージは、以下のような形式で送信されます。

☞**送信メールの例**

タイトル:Rooster IP Report
送信者:Rooster（004053010203） ⇒カッコ内は Rooster-LS の MAC アドレス
内容:Rooster IP-Address Report v0.01.
MAC=004053010203 ⇒Rooster-LSのMACアドレス
IP=10.20.30.40 ⇒割り当てられるグローバルIPアドレス

文字列を指定して入力を行う場合、指定のメッセージ入力フォームに、“%s” (”は不要)と入力すると、取得したグローバルIPアドレスに変換されて通知されます。
※割り当てグローバルIPアドレスが”11.22.33.44”の場合。

設定内容	実際に送信されるメッセージ
http://%s/mobile	http://11.22.33.44/mobile

2. 設定 ボタンをクリックして、設定内容を反映させます。

7.1.2 ダイナミックDNSサービスを利用する設定

1. 「ダイナミック DNS サービスを利用する。」のチェックをオンにし、以下の設定を行います。

■ **更新時間の間隔**

指定されたダイナミックDNSサービスへ、設定された時間ごとに更新を行います。
“0”を設定した場合自動更新となり、グローバルIPアドレスが変更された時のみ、ダイナミックDNSサービスへの更新を行います。
“0”以外を設定される場合、設定の最小値は5（分）となります。

■ **サービスの種類**

「suncomm.DDNS」のみの設定です。

> **注意** ダイナミック DNS サービスを使用される場合は、別途契約または登録が必要となります。詳細につきましては、下記の URL をご覧ください。
>
> ● **「suncomm.DDNS」**
>
> http://www.sun-denshi.co.jp/sc/ddns/index.html
> サン電子㈱が運用する有償でのダイナミックDNSサービスです。
> 別途、ご契約が必要となりますので、上記URLをご参照ください。
> また、「suncomm.DDNS」機能を利用して、お客様独自にダイナミックDNSサーバを設置・運用いただくことも可能です。
> 「suncomm.DDNS」のプロトコル仕様につきましては、機密保持契約成立後、開示させていただきます。なお、本件は法人のお客様に限らせていただきます。

［サーバ名］、［ホスト名］、［アカウント］、［パスワード］を入力します。

2. 設定 ボタンをクリックして、設定内容を反映させます。

7.2 DNSサービス

1. 設定ツールのメニューから、[各種サービス]－[DNS サービス]をクリックします。

「DNSサービス」設定のページが表示されます。

各種サービス

各種サービスの設定を行います。

DNSサービス

DNSリレー機能の設定を行います。

☑ DNSリレー機能を使用する。

設定

図 7-3　　DNS サービス設定画面

2. DNS リレー機能を使用する場合、「DNS リレー機能を使用する。」チェックをオンにします。
3. 設定 ボタンをクリックして、設定内容を反映させます。

- DNS リレー機能を使用するかしないかによって、接続機器 TCP/IP 設定の DNS サーバ設定方法が異なってきます。以下のうち該当する設定を行ってください。

DNS リレー機能を使用する場合。

⇒下記のいずれかの設定を行います。

- DNS サーバアドレスを自動的に取得するように設定します。
- DNS サーバアドレスを指定する場合、Rooster-LS の LAN IP アドレス、またはプロバイダ指定の DNS サーバ(ネームサーバ)アドレスを指定します。

DNS リレー機能を使用しない設定の場合。

⇒自動取得されないので、指定する必要があります。
プロバイダ指定のDNSサーバ(ネームサーバ)アドレスを指定します。

7.3 DHCPサービス

1. 設定ツールのメニューから、[各種サービス]－[DHCP サービス]をクリックします。

「DHCPサービス」設定のページが表示されます。

各種サービス

各種サービスの設定を行います。

DHCPサービス

DHCP機能の設定を行います。

図 7-4　　DHCP サービス設定画面

2. DHCP 機能を使用する場合、「DHCP 機能を使用する。」チェックをオンにします。
3. DHCP 機能の[方式]として「DHCP サーバ」、「DHCP リレー」のいずれかを選択します。

■ **「DHCP サーバ」を選択した場合**

Rooster-LS自身をDHCPサーバとして動作させたい場合に設定します。
[リース開始IPアドレス]に、割り当てるIPアドレスの開始アドレスを入力します。[個数]に、DHCPサーバ機能で使用する、リース開始IPアドレスからのアドレスの個数を指定します。
初期設定では、[リース開始IPアドレス]が「192.168.62.50」、[個数]が「50」と設定されているので、「192.168.62.50～192.168.62.99」が、DHCPサーバ機能で使用するIPアドレスの範囲となります。

■ **「DHCP リレー」を選択した場合**

Rooster-LS以外の機器をDHCPサーバとして動作させたい場合に設定します。
[上位DHCPサーバIPアドレス]に、DHCPサーバとして動作させる機器のIPアドレスを入力します。

4. 設定 ボタンをクリックして、設定内容を反映させます。

Rooster-LSのDHCPテーブルは、設定ツールのメニューから、[ステータス]－[DHCP割り当て一覧]をクリックして表示される「DHCP割り当て表示画面」から確認することができます。

ステータス

現在の設定・状態を表示します。

DHCP割り当て

DHCP割り当て一覧を表示します。

再読込

No.	IPアドレス	MACアドレス
1	192.168.62.50	[illegible]

図 7-5　　DHCP 割り当て表示画面

■　**IP アドレス**

Rooster-LS LAN内にあるLAN接続機器に割り当てたIPアドレスが表示されます。

■　**MAC アドレス**

上記のIPアドレスを付与された、LAN接続機器のMACアドレスが表示されます。

注意

Rooster-LS を再起動すると、DHCP テーブルはすべてリセットされます。

再起動後、クライアントからの IP アドレス割り当て要求を受けたタイミングで、再度 DHCP テーブルに登録されます。

7.4　TELNETサービス

- TELNET サービスによって、Web 設定ツールで設定可能なすべての項目を設定できます。
（設定ツールで行えない設定も一部可能です。）
- TELNET コマンドの詳細は、弊社ホームページより「Rooster-LS TELNET 設定機能取扱説明書」をダウンロードし、ご参照ください。

1. 設定ツールのメニューから、[各種サービス]－[TELNET サービス]をクリックします。

「TELNETサービス」設定のページが表示されます。

図 7-6　　TELNET サービス設定画面

2. TELNET サービスを使用する場合、「TELNET サービスを使用する。」チェックをオンにします。
3. [ポート番号]で、TELNET サービスで使用するポート番号を入力します。
4. 以下の設定を行います。

■　**LAN ポートからのアクセスを許可する。**

チェックをオンにすると、LAN1･2ポートからのTELNETログインができます。
オフにすると、LAN1･2ポートからのTELNETログインを拒否します。

■　**外部からのアクセス**

WAN側からのTELNETログイン（設定ツールへのログイン）を許可するポリシーを設定します。
[許可しない]、[全て許可する]、[INPUTフィルタリングに従う]から選択します。

5. 設定 ボタンをクリックして、設定内容を反映させます。

7.5 Webサービス

※メモ Web サービスについて

Web サービスは、Rooster-LS の設定ツールにアクセスを行う機能です。

設定によりLANポートまたはWANから設定ツールにアクセスできるポートを決定することができます。

1. 設定ツールのメニューから、[各種サービス]－[Web サービス]をクリックします。
「Webサービス」設定のページが表示されます。

図 7-7　　Web サービス設定画面

2. Web サービスを使用する場合、「Web サービスを使用する。」チェックをオンにします。
3. [ポート番号]で、Web サービスで使用するポート番号を入力します。
4. 以下の設定を行います。

■ **LAN ポートからのアクセスを許可する。**

チェックをオンにすると、LAN1･2ポートからの設定ツールへのログインができます。
オフにすると、LAN1･2ポートから設定ツールへのログインを拒否します。

■ **外部からのアクセス**

WAN側からの設定ツールへのログインを許可するポリシーを設定します。
[許可しない]、[全て許可する]、[INPUTフィルタリングに従う]から選択します。

5. 設定 ボタンをクリックして、設定内容を反映させます。

7.6 QoS

※メモ QoS 機能について

QoS(Quality of Service)とは、ネットワーク上で、ある特定の通信のための帯域を予約し、一定の通信速度を保証する技術のことをいいます。

Rooster-LS では、送信元、相手先 IP アドレスとポート番号で通信を特定し、その通信の帯域を確保することができます。

- QoS の設定は、以下の図の〇の方向への通信に適用されます。

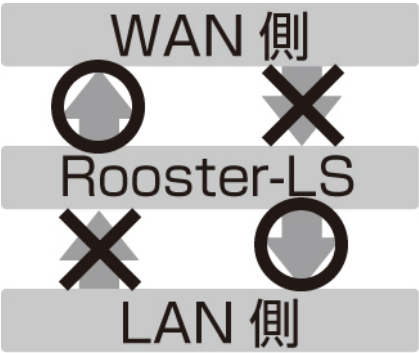



図 7-8　　QoS の適用範囲

1. 設定ツールのメニューから、[各種サービス]－[QoS]をクリックします。
「QoS設定リスト」のページが表示されます。

各種サービス

各種サービスの設定を行います。

QoS

QoS機能の設定を行います。

QoS設定の追加 追加

No.	帯域幅	送信元IP	送信元ポート番号	宛先IP	宛先ポート番号	メモ	操作
1	64 kbps	11.22.33.44	8080	22.33.44.55	8081	QoS	変更 削除

図 7-9　　QoS 機能設定画面

2. QoS 機能を使用する場合、「QoS 機能を使用する。」チェックをオンにします。
3. [全体の帯域幅]に、接続を行うサービスの帯域の理論値を入力します。
例）128k パケット通信サービスの場合、“128”と入力します。
4. 設定 ボタンをクリックして、設定内容を反映させます。

注意 QoS 機能の追加を行う前に、ここで一度、設定 ボタンをクリックして、設定内容を反映させます。
先に 追加 ボタンをクリックすると、設定した内容が破棄されてしまいます。

7.6.1 QoS機能の追加設定

5. QoS 機能の追加を行う場合は、追加 ボタンをクリックします。
   既存の設定を変更する場合は、[変更]をクリックします。

   [削除]をクリックすると、表示されている設定が削除されます。
   追加 ボタンまたは、[変更]をクリックすると、「QoS機能の詳細設定」ページが表示されます。
   追加 ボタンをクリックした場合は空白の状態で、[変更]をクリックした場合は、設定済みの情報が入力された状態で開きます。

メモ
- QoS 機能の設定は最大 8 件まで行えます。
- 設定が適用される優先順位は、No の昇順となり、No.1 が一番高い優先順位となります。

図 7-10 QoS 機能詳細設定画面

6. 以下の設定を行います。

■ **No.**

QoS機能設定の通し番号が表示されます。

■ **宛先インターフェイス**

この設定を適用するインターフェイスを選択します。
[LAN]、[モバイル通信端末]のいずれかを指定します。

■ **帯域幅**

設定を行う通信に割り当てる帯域を設定します。

■ **送信元 IP**

設定を行う通信の送信元IPアドレスを設定します。
入力がない場合、すべての送信元に設定が適用されます。

■ **送信元ポート番号**

設定を行う通信の送信元ポート番号を設定します。
入力がない場合、すべてのポート番号に設定が適用されます。

■ **宛先 IP**

設定を行う通信の宛先IPアドレスを設定します。
入力がない場合、すべての宛先に設定が適用されます。

■ **宛先ポート番号**

設定を行う通信の宛先ポート番号を設定します。
入力がない場合、すべてのポート番号に設定が適用されます。

■ **メモ**

設定内容を分かりやすくするための覚え書きを入力します。
半角16文字（全角8文字）までの任意の文字列を入力できます。

7. 設定 ボタンをクリックすると、「QoS 設定リスト」のページに戻り、設定した内容が反映されます。
   キャンセル ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じます。

QoS 機能は、設定された帯域を必ず保証するものではありません。
実回線速度が遅い場合、設定された帯域通りに確保できない場合がございます。

7.7 SNMP

SNMP について

SNMP（Simple Network Management Protocol）は、ネットワーク機器の状態をネットワーク経由で問い合わせたり、それに答えたりするための通信手順の一つをいいます。

SNMP を使用することによって、ネットワーク管理を容易に行うことができるようになります。

SNMP コミュニティは、監視する側のネットワーク監視端末（SNMP マネージャ）と、監視される側のネットワーク上の機器（SNMP エージェント）により構成され、このうち Rooster-LS は、SNMP エージェントとしての動作に対応しております。

対応バージョンは、SNMPv1 のみとなります。

1. 設定ツールのメニューから、[各種サービス]－[SNMP]をクリックします。

「SNMP」設定のページが表示されます。

各種サービス

各種サービスの設定を行います。

SNMPサービス

SNMPサービスの設定を行います。

☑ SNMPサービスを使用する。

SNMPマネージャIPアドレス: 192.168.62.50

（未設定時は、すべてのIPアドレスからのアクセスを許可する。）

コミュニティ名: public

SYSLocation名: suncomm

☑ SNMP TRAPを使用する。

☑ LANポートからのアクセスを許可する。

☐ 外部からのアクセスを許可する。

[設定]

図 7-11 SNMP サービス設定画面

2. SNMP 機能を使用する場合、「SNMP 機能を使用する。」チェックをオンにします。
3. 以下の設定を行います。

■ **SNMP マネージャ IP アドレス**

SNMPマネージャのローカルIPアドレスを設定します。

■ **コミュニティ名**

SNMPマネージャとRooster-LSがやり取りを行うためのコミュニティ名を設定します。最大16文字まで設定できます。

■ **SYSLocation 名**

MIB変数のSYSLocation名を設定します。

■ **SNMP TRAP を使用する**

Rooster-LSから、SNMPマネージャIPアドレス宛に SNMP TRAPを送信する場合、チェックをオンにします。

■ **LAN ポートからのアクセスを許可する。**

チェックをオンにすると、LAN1･2ポートからのアクセスができます。
オフにすると、LAN1･2ポートからのアクセスができません。

■ **外部からのアクセスを許可する。**

チェックをオンにすると、WAN側からのアクセスができます。
オフにすると、WAN側からのアクセスができません。

4. [設定] ボタンをクリックして、設定内容を反映させます。

7.8 WANハートビート機能

> **※メモ　WAN ハートビート機能について**
>
> WAN ハートビート機能は、WAN 側のネットワークに正常にアクセスできるか、WAN 側のインターフェイスが正常に動作しているかの確認を行うための機能です。

1. 設定ツールのメニューから、[各種サービス]－[WAN ハートビート]をクリックします。

「WANハートビート」設定のページが表示されます。

各種サービス

各種サービスの設定を行います。

WANハートビート

WANハートビートの設定を行います。

☑ WANハートビートを使用する。

監視時間: 1 分

10 回連続無応答時の動作: ○ 本機をリセットする。 ◉ ログに記録のみ。

監視先ホストの指定

○ WANのゲートウェイ

◉ 手動設定する: 192.168.1.1 ☑ VPN接続先

設定

図 7-12　WAN ハートビート設定画面

2. WAN ハートビートを使用する場合、「WAN ハートビートを使用する。」のチェックをオンにします。
3. 以下の設定を行います。

■ **監視時間**

設定された間隔でWANハートビートを実行します。
“0”を設定した場合、Rooster-LS再起動直後のみWANハートビートを実行します。“0”以外を設定される場合、設定の最小値は1(分)となります。

■ **無応答時の動作**

WANハートビートで、接続状態の確認ができなかった場合に行う動作を選択します。

- **無応答が連続して発生した場合、本機をリセットする。**
  指定した無応答回数分、連続で失敗した時点で、Rooster-LS を再起動します。
- **WAN ハートビートログを記録する。**
  再起動は行わず、設定された監視時間ごとに WAN ハートビートログに“失敗”のログを記録します。

■ **監視先 IP アドレスの指定**

WANハートビートを行う相手先を指定します。相手先IPアドレスを手動で設定することもできます。
指定するIPアドレスがVPN先ネットワークアドレスの場合は「VPN接続先」のチェックをオンにします。

> **※メモ**　「VPN 接続先」の設定は、ファームウェアバージョン:Version4.00 から実装された項目です。

4. [設定] ボタンをクリックして、設定内容を反映させます。

> **注意**
>
> - 従量制課金でご契約の場合は、設定しないようにしてください。
>   **意図しない接続で通信料金が掛かってしまう原因となりますので、くれぐれもご注意願います。**
> - WAN 側のゲートウェイ機器の仕様により、WAN ハートビートによる ping に応答しない場合があります。
>   ping に応答しない場合は手動設定にて IP アドレスを入力するか、WAN ハートビートログを記録するを選択ください。
> - WAN ハートビート機能は、以下の理由により無通信監視時間（☞4.3 ダイヤルアップ接続設定をご覧ください）の設定と併用できません。
>   - （無通信監視時間）＜（WAN ハートビート監視時間）の場合無通信監視時間で一旦切断されても、WAN ハートビートで再度、自動発信を行ってしまいます。
>   - （無通信監視時間）＞（WAN ハートビート監視時間）の場合無通信監視時間で切断される前に、WAN ハートビートの通信により無通信状態がリセットされてしまい切断されません。

7.9 ログ管理

1. 設定ツールのメニューから、[各種サービス]－[ログ管理]をクリックします。

「ログ管理」設定のページが表示されます。

各種サービス

各種サービスの設定を行います。

ログ管理

ログ管理機能の設定を行います。

☑ パケット通信ログを記録する。

☐ Syslogサーバに送信する。

Syslogサーバ IPアドレス：

☑ PPPログを記録する。

☐ USBログを記録する。

[設定]

図 7-13　ログ管理機能設定画面

2. 「パケット通信ログを記録する。」のチェックをオンにすると、[ログ]－[パケット通信ログ]の[通過ログ]、[遮断ログ]が有効になります。
   パケット通信ログの詳細は、☞ 9.1.1 パケット通過ログまたは☞9.1.2 パケット遮断ログをご覧ください。
3. Syslog サーバでログ管理を行いたい場合、「Syslog サーバに送信する。」のチェックをオンにし、Syslog サーバのローカル IP アドレスを入力します。
   この設定を行った場合、Rooster-LS で取得できる全てのログを Syslog サーバへ送信します。
4. 「PPP ログを記録する。」のチェックをオンにすると[ログ]－[サービスログ]の[PPP ログ]が有効になります。
   PPP ログの詳細は、☞ 9.3.4 PPP ログをご覧ください。
5. 「USB ログを記録する。」のチェックをオンにすると、USB ポートに接続した USB メモリに Rooster-LS で取得できる全てのログを記録します。

注意

- USB メモリを抜き差しする場合は Rooster-LS の電源が切れている時に行ってください。電源が入っている時は USB メモリを抜き差ししないでください。なお、USB ハブは使用できません。
- USB メモリの種類によっては動作しないものがあります。必ず USB ランプが点灯すること、ログが正しく保存されることを確認ください。

6. [設定] ボタンをクリックして、設定内容を反映させます。

8. ネットワーク設定

8.1 VPNパススルー

メモ　VPN パススルーについて

VPN パススルーの設定を行うと、Rooster-LS 以外の別の端末が VPN サーバやクライアントとして動作する時、各 VPN プロトコルを通過させることができるようになります。

VPN パススルーは 1 セッションのみとなります。

1. 設定ツールのメニューから、[ネットワーク]－[パススルー]をクリックします。

「VPNパススルー」設定のページが表示されます。

ネットワーク

ネットワークの各設定を行います。

パススルー

VPNパススルーの設定を行います。

☑ IPSecパススルーを使用する。

☑ PPTPパススルーを使用する。

[設定]

図 8-1　VPN パススルー設定画面

2. 通過させる VPN プロトコルのチェックをオンにします。
3. [設定] ボタンをクリックして、設定内容を反映させます。

8.2 スタティックルーティング

1. 設定ツールのメニューから、[ネットワーク]－[スタティックルーティング]をクリックします。
「スタティックルーティング」リストのページが表示されます。

ネットワーク

ネットワークの各設定を行います。

スタティックルーティング

スタティックルーティングの設定を行います。

設定の追加 追加

ID	ネットワーク	サブネットマスク	ゲートウェイ	インターフェイス	メモ	操作
1	11.22.33.44	255.255.255.0	192.168.62.100	LAN	static	変更 削除

図 8-2　　スタティックルーティングリスト画面

2. スタティックルートの追加を行いたい場合は、 追加 ボタンをクリックします。
設定済みのスタティックルーティング設定を変更する場合は、[変更]をクリックします。
[削除]をクリックすると、表示されている設定が削除されます。

追加 ボタンまたは、[変更]をクリックすると、「スタティックルーティングの詳細設定」ページが表示されます。
追加 ボタンをクリックした場合は空白の状態で、[変更]をクリックした場合は、設定済みの情報が入力された状態で開きます。

メモ スタティックルートの設定は最大 32 件まで行えます。

スタティックルーティングの詳細設定

No.	1
ネットワーク	11.22.33.44
サブネットマスク	255.255.255.0
ゲートウェイ	192.168.62.100
インターフェイス	LAN
メモ	static

設定 キャンセル

図 8-3　　スタティックルーティング詳細設定画面

3. 以下の設定を行います。

■ **ネットワーク**

宛先ネットワークアドレスを入力します。

■ **サブネットマスク**

上記ネットワークのサブネットマスクを入力します。

■ **ゲートウェイ**

上記ネットワークのゲートウェイアドレスを入力します。

■ **インターフェイス**

この設定を適用するインターフェイスを選択します。
[LAN]、[VPN]のいずれかを選択します。

メモ インターフェイスの選択はファームウェアバージョン：Version4.00 から実装されたものです。

■ **メモ**

設定内容を分かりやすくするための覚え書きを入力します。
半角16文字（全角8文字）までの任意の文字列を入力できます。

4. 設定 ボタンをクリックすると、「スタティックルーティング」リストのページに戻り、設定した内容が反映されます。
キャンセル ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「スタティックルーティング」リストのページに戻ります。

8.3 FORWARDフィルタリング

1. 設定ツールのメニューから、[ネットワーク]－[フィルタリング]－[FORWARD]をクリックします。

「FORWARDフィルタリング」リストのページが表示されます。

ネットワーク

ネットワークの各設定を行います。

FORWARDフィルタリング

FORWARDフィルタリングの設定を行います。

基本ポリシー 設定されていないパケットはすべて遮断する。 設定

設定の追加 追加

工場出荷時状態に戻す 初期化

No.	インターフェイス	方向	動作	プロトコル	相手IPアドレス	相手ポート	メモ	操作
1	全て	送信	許可	TCP		80 - 80	HTTP	変更 削除
2	全て	送信	許可	UDP		53 - 53	DNS	変更 削除
3	全て	送信	許可	TCP		25 - 25	SMTP	変更 削除
4	全て	送信	許可	TCP		110 - 110	POP3	変更 削除
5	全て	送信	許可	TCP		1720 - 1720	NetMeeting	変更 削除
6	全て	送信	許可	TCP		1503 - 1503	NetMeeting	変更 削除
7	全て	送信	許可	TCP		443 - 443	SSL	変更 削除
8	全て	送信	許可	ICMP		-	ICMP	変更 削除
9	全て	送信	許可	TCP		21 - 21	FTP	変更 削除
10	全て	送信	許可	UDP		123 - 123	NTP	変更 削除
11	全て	送信	許可	TCP		23 - 23	TELNET	変更 削除
12	全て	受信	許可	TCP		23 - 23	TELNET	変更 削除
13	全て	受信	許可	TCP		80 - 80	HTTP	変更 削除
14	全て	受信	許可	TCP		21 - 21	FTP	変更 削除
15	全て	受信	許可	ICMP		-	ICMP	変更 削除
16	全て	送信	許可	TCP		587 - 587	OP25B	変更 削除

図 8-4　　FORWARD フィルタリング設定リスト画面

2. FORWARD フィルタリング設定を行った項目以外のパケットをどう処理するかにより、「基本ポリシー」の

- **「設定されていないパケットはすべて通す。」**
- **「設定されていないパケットはすべて遮断する。」**

のうちいずれかを選択します。

注意

- 設定済みの項目につきましては、「基本ポリシー」の設定に関わらず、個別に設定した動作が適用されます。
- VPN 間の通信は、この設定に関わらず、基本ポリシーは「すべて通す」設定で固定となります。
（VPN 設定の詳細は、☞ 8.7 VPN 設定をご覧ください）

3. FORWARD フィルタリング設定の追加を行いたい場合は、[追加] ボタンをクリックします。
設定済みの FORWARD フィルタリング設定を変更する場合は、[変更]をクリックします。[削除]をクリックすると、表示されている設定が削除されます。

[追加] ボタンまたは、[変更]をクリックすると、「FORWARDフィルタリングの詳細設定」ページが表示されます。

[追加] ボタンをクリックした場合は空白の状態で、[変更]をクリックした場合は、設定済みの情報が入力された状態で開きます。

メモ FORWARD フィルタリングの設定は最大 32 件まで行えます。

FORWARDフィルタリングの詳細設定

No.	17
インターフェイス	全て
方向	送信
動作	許可
プロトコル	TCP
プロトコル番号	
相手IPアドレス	11.22.33.44
相手ポート	8080 – 8080
メモ	WEB

設定　キャンセル

図 8-5　　FORWARD フィルタリング詳細設定画面

4. 以下の設定を行います。

- **No.**

FORWARDフィルタリング設定の通し番号が表示されます。

- **インターフェイス**

この設定を適用するインターフェイスを選択します。[全て]のみ。

■ **方向**

[受信]、[送信]のいずれかを指定します。

■ **動作**

[許可]、[遮断]のいずれかを指定します。

■ **プロトコル**

[全て]、[UDP]、[TCP]、[ICMP]、[ユーザ指定]のいずれかを指定します。
[ユーザ指定]の場合は、プロトコル番号も指定します。

■ **プロトコル番号**

[プロトコル]にて「ユーザ指定」を選択した場合は、プロトコル番号を設定します。

■ **相手 IP アドレス**

FORWARDフィルタリングを行う宛先IPアドレスを設定します。

■ **相手ポート**

FORWARDフィルタリングを行うポート番号を、1～65535の番号で範囲指定します。

■ **メモ**

設定内容を分かりやすくするための覚え書きを入力します。半角16文字 (全角8文字)までの任意の文字列を入力できます。

5. [設定] ボタンをクリックすると、「FORWARD フィルタリング」リストのページに戻り、設定した内容が反映されます。
   [キャンセル] ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「FORWARD フィルタリング」のリストのページに戻ります。

FORWARD フィルタリング設定を工場出荷時の状態に戻す場合は、[初期化]ボタンを押すか、下記の表をご参照いただき、フィルタリングの再設定を行ってください。

表 8-1　工場出荷時の FORWARD フィルタリングの設定

No.	I/F	方向	動作	プロトコル	相手 IP アドレス	相手ポート	メモ
1	全て	送信	許可	TCP		80-80	HTTP
2	全て	送信	許可	UDP		53-53	DNS
3	全て	送信	許可	TCP		25-25	SMTP
4	全て	送信	許可	TCP		110-110	POP3
5	全て	送信	許可	TCP		1720-1720	NetMeeting
6	全て	送信	許可	TCP		1503-1503	NetMeeting
7	全て	送信	許可	TCP		443-443	SSL
8	全て	送信	許可	ICMP		-	ICMP
9	全て	送信	許可	TCP		21-21	FTP
10	全て	送信	許可	UDP		123-123	NTP
11	全て	送信	許可	TCP		23-23	TELNET
12	全て	受信	許可	TCP		23-23	TELNET
13	全て	受信	許可	TCP		80-80	HTTP
14	全て	受信	許可	TCP		21-21	FTP
15	全て	受信	許可	ICMP		─	ICMP
16	全て	送信	許可	TCP		587-587	OP25B

工場出荷時では、表 8-1 以外はすべて遮断されます。

それ以外のプロトコルを通過させたい場合は、新たにフィルタリングの設定を行う必要があります。

8.4 INPUTフィルタリング

設定ツールのメニューから[ネットワーク]－[フィルタリング]－[INPUT]をクリックします。
「INPUTフィルタリング」リストのページが表示されます。

ネットワーク

ネットワークの各設定を行います。

INPUTフィルタリング

INPUTフィルタリングの設定を行います。

設定の追加 [追加]

No.	動作	プロトコル	相手IPアドレス	ネットマスク	相手ポート	メモ	操作
1	許可	TCP	11.22.33.44	255.255.255.254	8080 - 8080	WEB	変更 削除

図 8-6　INPUT フィルタリング設定リスト画面

8.4.1　INPUTフィルタリングの追加設定

1. INPUT フィルタリングの追加を行う場合は、[追加] ボタンをクリックします。
   既存の設定を変更する場合は、[変更]をクリックします。

   [削除]をクリックすると、表示されている設定が削除されます。
   [追加] ボタンまたは、[変更]をクリックすると、「INPUTフィルタリングの詳細設定」ページが表示されます。
   [追加] ボタンをクリックした場合は空白の状態で、[変更]をクリックした場合は、設定済みの情報が入力された状態で開きます。

> メモ　INPUT フィルタリングの設定は最大 64 件まで行えます。

INPUTフィルタリングの詳細設定

No.	1
動作	許可
プロトコル	TCP
相手IPアドレス	11.22.33.44
ネットマスク	255.255.255.254
相手ポート	8080 – 8080
メモ	WEB

[設定] [キャンセル]

図 8-7　　INPUT フィルタリング詳細設定画面

2. 以下の設定を行います。

■ **No.**

INPUTフィルタリング設定の通し番号が表示されます。

■ **動作**

INPUTフィルタリングの動作を指定します。[許可]のみ。

■ **プロトコル**

[UDP]、[TCP]のいずれかを指定します。

■ **相手 IP アドレス**

INPUTフィルタリングを行う相手IPアドレスを設定します。

■ **ネットマスク**

INPUTフィルタリングを行う相手サブネットマスクを指定します。

■ **相手ポート**

INPUTフィルタリングを行うポート番号を、1～65535の番号で範囲指定します。

■ **メモ**

設定内容を分かりやすくするための覚え書きを入力します。半角16文字（全角8文字）までの任意の文字列を入力できます。

3. [設定] ボタンをクリックすると、「INPUT フィルタリング」リストのページに戻り、設定した内容が反映されます。
   [キャンセル] ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「INPUT フィルタリング」のリストのページに戻ります。

8.5　バーチャルサーバ

> メモ　**バーチャルサーバ機能について**
>
> バーチャルサーバ機能は、インターネット上（リモートホスト）から、LAN 側の接続機器にアクセスを行わせる際に設定する機能です。
>
> 通常、LAN に設置されている機器は、ローカル IP アドレスを持っており、グローバル IP アドレスでアクセスを行うことはできません。
>
> バーチャルサーバ機能を利用し、プロトコル・TCP/UDP ポート番号を指定することによって、LAN 内のどの接続機器へ向けての通信であるか特定できるようになるため、グローバル IP アドレスからのアクセスが行えるようになります。
>
> DMZ と同時に使用することは出来ません。

1. 設定ツールのメニューから、[ネットワーク]－[バーチャルサーバ]をクリックします。
   「バーチャルサーバ」リストのページが表示されます。

ネットワーク

ネットワークの各設定を行います。

バーチャルサーバ

バーチャルサーバの設定を行います。

設定の追加 [追加]

No.	インターフェイス	プロトコル	ポート番号	サーバのIPアドレス	メモ	操作
1	モバイル通信端末	TCP	80	192.168.62.100	http	変更 削除

図 8-8　　バーチャルサーバ設定リスト画面

2. バーチャルサーバ設定の追加を行いたい場合は、[追加] ボタンをクリックします。設定済みの項目を変更する場合は、[変更]をクリックします。
   [削除]をクリックすると、表示されている設定が削除されます。
   [追加] ボタンまたは、[変更]をクリックすると、「バーチャルサーバの詳細設定」ページが表示されます。
   [追加] ボタンをクリックした場合は空白の状態で、[変更]をクリックした場合は、設定済みの情報が入力された状態で開きます。

メモ　バーチャルサーバの設定は最大 16 件まで行えます。

バーチャルサーバの詳細設定

No.	1
インターフェイス	モバイル通信端末
プロトコル	TCP
ポート番号	80
サーバのIPアドレス	192.168.62.50
サーバのポート番号	85
外部からのアクセス	INPUTフィルタリングに従う
メモ	http

[設定] [キャンセル]

図 8-9　　バーチャルサーバ設定画面

3. 以下の設定を行います。

■ **No.**

バーチャルサーバ設定の通し番号が表示されます。

■ **インターフェイス**

バーチャルサーバの設定を行うインターフェイスを指定します。
指定できるのは、[モバイル通信端末]のみとなります。

■ **プロトコル**

[TCP]、[UDP]のいずれかを指定します。

■ **ポート番号**

WAN側で受け付けるポート番号を、1～65535 までの番号で指定します。
"＊" などのワイルドカードでの指定は行えません。

■ **サーバの IP アドレス**

バーチャルサーバとして外部に公開する機器のIPアドレスを指定します。

■ **サーバのポート番号**

LAN側のサーバに転送するポート番号を、1～65535までの番号で指定します。指定しない場合は「ポート番号」と同じポート番号となります。

■ **外部からのアクセス**

WAN側からのサーバへのアクセスを許可するポリシーを設定します。
[全て許可する]、[INPUTフィルタリングに従う]から選択します。

■ **メモ**

設定内容を分かりやすくするための覚え書きを入力します。半角16文字 (全角8文字)までの任意の文字列を入力できます。

4. [設定] ボタンをクリックすると、「バーチャルサーバ」リストのページに戻り、設定した内容が反映されます。
   [キャンセル] ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「バーチャルサーバ」のリストのページに戻ります。

8.6 DMZ

メモ **DMZ 機能について**

DMZ 機能は、バーチャルサーバ機能と同様、インターネット上(リモートホスト)から、LAN 側の接続機器にアクセスを行わせる際に設定する機能ですが、ポート番号が不明な場合でも設定できます。

ポート番号が特定できない通信を行いたい場合などに最適な設定です。ただし、以下の点にご注意願います。

- Rooster-LS では、DMZ として設定できる機器は一台のみとなります。
- DMZ として設定された機器には、フィルタリングの設定が(詳細は、☞ 8.3 FORWARD フィルタリング 8.4 INPUT フィルタリングをご覧ください。)全く適用されなくなり、セキュリティが弱くなります。
  必要な場合のみ設定を行うようにしてください。

バーチャルサーバと同時に使用することは出来ません。

1. 設定ツールのメニューから、[ネットワーク]－[DMZ]をクリックします。

「DMZ」設定のページが表示されます。

ネットワーク

ネットワークの各設定を行います。

DMZ

DMZの設定を行います。

☑DMZを使用する。

DMZを使用する機器のプライベートIPアドレス：192.168.62.200

[設定]

図 8-10　DMZ 設定画面

2. DMZ を使用する場合、「DMZ を使用する。」のチェックをオンにします。
3. 「DMZ を使用する機器のプライベート IP アドレス」に、DMZ として設定する機器のプライベート IP アドレスを入力します。
4. [設定] ボタンをクリックして、設定内容を反映させます。

8.7 VPN設定

メモ　VPN について

VPN（Virtual Private Network）は、データのカプセル化や暗号化などのセキュリティ技術を使って、インターネットなどの公共的なネットワークで、あたかも専用線接続のような、秘匿性の高いネットワークを実現させるためのしくみです。

Rooster-LS では、IPsec（Security Architecture for Internet Protocol）によるインターネット VPN の構築を行うことができます。

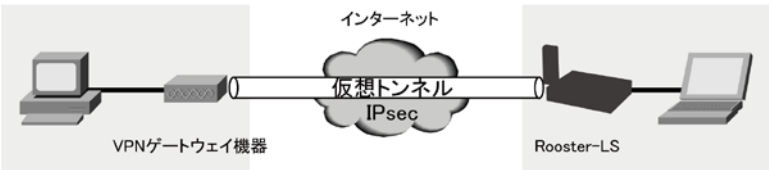



図 8-11　VPN による接続概要図

5. 設定ツールのメニューから、[ネットワーク]－[VPN]をクリックします。

「VPN」リストのページが表示されます。

ネットワーク

ネットワークの各設定を行います。

VPN

VPNの設定を行います。

設定の追加 [追加]

No.	プロトコル	インターフェイス	相手IPアドレス	相手ネットワーク	メモ	操作
1	IPsec	モバイル通信端末	11.22.33.44	192.168.65.0	VPN	変更 削除

図 8-12　VPN 設定リスト画面

6. VPN 設定の追加を行いたい場合は、[追加] ボタンをクリックします。設定済みの項目を変更する場合は、[変更]をクリックします。

「VPNの詳細設定」ページが表示されます。

メモ VPN の設定は最大 16 件まで行えます。

VPNの詳細設定

No.	1
プロトコル	IPsec
インターフェイス	モバイル通信端末
モード設定	メインモード
接続種別	イニシエータ
ハッシュアルゴリズム	SHA-1
暗号化アルゴリズム	3DES
PreSharedKey	test
IKE Life Time	3600 秒
IPsec Life Time	28800 秒
相手IPアドレス	11.22.33.44
相手ネットワーク	192.168.61.0
相手ネットマスク	255.255.255.0
相手側識別子	
Rooster側IPアドレス	
Rooster側ネットワーク	
Rooster側ネットマスク	
Rooster側識別子	
メモ	

☐セッションキープを行う。

☐キープアライブを行う。

監視先IPアドレス1

監視先IPアドレス2

☐バックアップ設定を使用する。

バックアップ設定

設定　キャンセル

図 8-13　VPN 設定画面

7. 以下の設定を行います。

■ **No.**

VPN設定の通し番号が表示されます。

■ **プロトコル**

対応プロトコルはIPsecのみで固定となります。

■ **インターフェイス**

この設定を適用するインターフェイスを選択します。
[モバイル通信端末]のみ設定できます。

■ **モード設定**

「メインモード」、あるいは「アグレッシブモード」を選択します。

■ **接続種別**

「イニシエータ」または「レスポンダ」のいずれかを選択します。
「イニシエータ」はIKE接続要求を行います。「レスポンダ」はIKEの待受けを行います。

■ **ハッシュアルゴリズム**

「SHA-1」または「MD5」のいずれかを選択します。
フェーズ1、フェーズ2とも共通の設定になります。

■ **暗号化アルゴリズム**

「AES256bit」または「3DES」のいずれかを選択します。

暗号化アルゴリズムの設定は、ファームウェアバージョン:Version4.00 から実装された項目です。

■ **PreSharedKey**

IPsec通信を行うために使用する認証用キーフレーズを設定します。
2点間で同じ値を設定します。

■ **IKE Life Time**

IKEの寿命を秒単位で指定します。1081秒以上で設定してください。

■ **IPsec Life Time**

IPsecの寿命を秒単位で指定します。1081秒以上で設定してください。

■ **相手 IP アドレス**

IPsec通信を行う相手先のグローバルIPアドレスを指定します。
ホスト名での指定も可能です。
モード設定が「アグレッシブ」で接続種別が「レスポンダ」の場合、相手IPアドレスには「0.0.0.0」と設定してください。

■ **相手ネットワーク**

IPsec通信を行う相手先のローカルネットワークアドレスを指定します。
（相手側ID）

■ **相手ネットマスク**

IPsec通信を行う相手先のローカル(サブ)ネットマスクアドレスを指定します。
(相手側ID)

■ **相手側識別子**

アグレッシブモードで接続する際に、IPsec通信で互いに相手を識別するために設定します。接続種別で「レスポンダ」を選択された場合に設定し、2点間で同じ値を設定します。「@」をはさんだ文字列にて指定します。例)test@test

■ **Rooster 側 IP アドレス**

メインモードで接続する際にRoosterに割り当てられるグローバルIPアドレスを指定します。ホスト名での指定も可能です。

■ **Rooster 側ネットワーク**

Roosterのローカルネットワークアドレスを指定します。
(Rooster側ID)

■ **Rooster 側ネットマスク**

Roosterのローカル(サブ)ネットマスクアドレスを指定します。
(Rooster側ID)

■ **Rooster 側識別子**

アグレッシブモードで接続する際に、IPsec通信で互いに相手を識別するために設定します。接続種別で「イニシエータ」を選択された場合に設定し、2点間で同じ値を設定します。「@」をはさんだ文字列にて指定します。例)test@test

■ **メモ**

設定内容を分かりやすくするための覚え書きを入力します。
半角16文字(全角8文字)までの任意の文字列を入力できます。

■ **セッションキープを行う**

チェックをオンにした場合、VPN接続が切断されると、自動的に再接続を行うようになります。接続種別で「レスポンダ」を選択された場合は、チェックをオンにしても動作いたしません。

■ **キープアライブを行う**

VPN接続を常時監視し、接続状態を続ける機能です。
チェックをオンにした場合、VPN接続時に接続確認のために、設定された監視先IPアドレスにpingパケットを発信するようになります。

注意 セッションキープ、キープアライブは、従量制課金でご契約の場合は、設定しないようにしてください。
意図しない接続で通信料金が掛かってしまう原因となりますので、くれぐれもご注意願います。

■ **バックアップ設定を使用する**

上記の設定で接続できなかった場合、代替の設定で接続を行うようにすることができます。代替の設定を使用する場合、チェックをオンにします。
接続種別が「レスポンダ」の場合、チェックをオンにしても動作いたしません。

注意 引き続いて「バックアップ設定」も行う場合は、ここで一度、[設定] ボタンをクリックして、設定内容を反映させます。
先にクリックすると、設定した内容が破棄されてしまいます。

8. [設定] ボタンをクリックすると、「VPN」リストのページに戻り、設定した内容が反映されます。
[キャンセル] ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「VPN」のリストのページに戻ります。

注意
- 設定が空白の場合、自動的に適切な設定が行われるようになっています。
- VPN の接続が完了するまでに1～3 分程度かかります。
通信を行う前に、ping コマンド等で接続状態を確認することをお勧めします。

● 他社製 VPN 機器と接続を行う場合、以下の表を参考に設定を行ってください。

表 8-2　Rooster-LS 既定の VPN 接続設定

項目	既定の設定内容
基本設定	
データ圧縮 (IPComp プロトコル)	圧縮は使用しない。
鍵交換方式	IKE(Internet Key Exchange)を使って、SA の合意を通信時に自動的に行う。 (手動設定は行わない。)
IKE フェーズ 1 (ISAKMP SA の作成) の設定	
接続試行回数	無限回(制限なし)
ハッシュアルゴリズム	SHA-1、MD5
認証方式	Pre-Shared Key (共通鍵) 認証方式
Pre-Shared Key (共通鍵) の設定	自分側と相手側両方に、同じキーフレーズを設定。
暗号化アルゴリズム	AES256bit、3DES
Diffie-Hellman-Group	DH Group 2
識別子 (ホスト ID)	「@」をはさんだ文字列
IKE Life Time	経過時間による設定のみ。
IKE フェーズ 2 (IPsec SA の作成) の設定	
セキュリティプロトコル	ESP のみ。
IPsec Life Time	経過時間による設定のみ。
カプセル化モード	トンネリングモード
暗号化アルゴリズム	AES256bit、3DES
ハッシュアルゴリズム	SHA-1、MD5
PFS (Diffie-Hellman の再計算)	行わない。

8.7.1　VPN通信の接続／切断方法

1. 設定ツールのメニューから、[ステータス]－[VPN] をクリックします。

VPNステータスのページが表示されます。

ステータス

現在の設定･状態を表示します。

VPN

VPN通信の状態を表示します。

No.	相手IPアドレス	相手ネットワーク	メモ	ステータス	操作
1		192.168.1.0		接続完了	切断 無効

図 8-14　VPN ステータス表示画面

■ **No.**

VPN設定の通し番号が表示されます。

■ **相手 IP アドレス**

IPsec通信を行う相手先のグローバルIPアドレスが表示されます。

■ **相手ネットワーク**

IPsec通信を行う相手先のローカルネットワークアドレスが表示されます。

■ **メモ**

メモに設定された文字列が表示されます。

■ **ステータス**

設定したVPNの現在の状態が表示されます。

● **ステータス一覧**

ステータス表示	状態	VPN ランプの状態
無効	VPN 設定が無効になっています。	消灯
待機中	VPN 接続設定は行われていますが、VPN 接続を試みていない状態です。	消灯
接続試行中	VPN 接続を行おうとしています。 この状態が長く続く場合、設定が間違っているか、相手側がオフラインになっている等の問題で接続できない可能性があります。	消灯
接続完了	VPN 接続が正常に行えた状態です。	点灯

■ **操作**

それぞれ以下の操作を行います。

- [接続]⇒接続動作を行います。
- [切断]⇒切断動作を行います。
- [無効]⇒設定を無効にします。
  次回、[有効]をクリックするまで設定内容を使えないようにします。
- [有効]⇒設定を有効にします。
  次回、[無効]になっている設定を再度使えるようにします。

8.7.2　2点間のWAN側IPアドレスが固定の場合

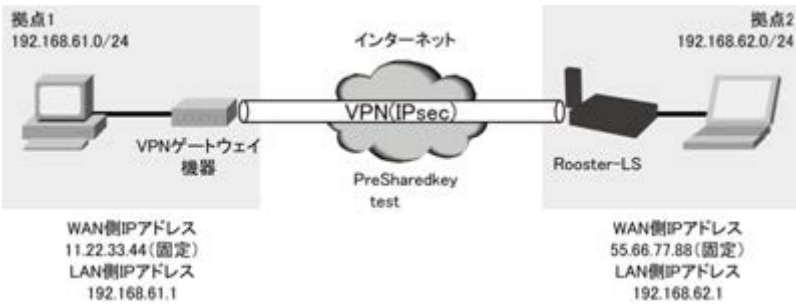



図 8-15　2 点間の WAN 側 IP アドレスが固定の場合

● Rooster-LS の設定例

VPNの詳細設定

項目	設定値
No.	1
プロトコル	IPsec
インターフェイス	モバイル通信端末
モード設定	メインモード
接続種別	イニシエータ
ハッシュアルゴリズム	SHA-1
暗号化アルゴリズム	3DES
PreSharedKey	test
IKE Life Time	3600 秒
IPsec Life Time	28800 秒
相手IPアドレス	11.22.33.44
相手ネットワーク	192.168.61.0
相手ネットマスク	255.255.255.0
相手側識別子	
Rooster側IPアドレス	
Rooster側ネットワーク	
Rooster側ネットマスク	
Rooster側識別子	
メモ	

☐ セッションキープを行う。
☐ キープアライブを行う。
監視先IPアドレス1
監視先IPアドレス2
☐ バックアップ設定を使用する。
バックアップ設定

[設定] [キャンセル]

図 8-16　Rooster-LS 側の設定

8.7.3　WAN側IPアドレスの一方が固定、Rooster-LSが動的の場合

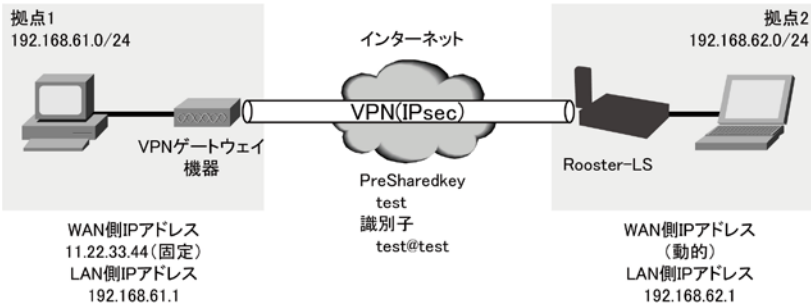



図 8-17　WAN 側 IP アドレスの一方が固定、Rooster-LS が動的の場合

● Rooster-LS の設定例

VPNの詳細設定

項目	設定値
No.	1
プロトコル	IPsec
インターフェイス	モバイル通信端末
モード設定	アグレッシブモード
接続種別	イニシエータ
ハッシュアルゴリズム	SHA-1
暗号化アルゴリズム	3DES
PreSharedKey	test
IKE Life Time	3600 秒
IPsec Life Time	28800 秒
相手IPアドレス	11.22.33.44
相手ネットワーク	192.168.61.0
相手ネットマスク	255.255.255.0
相手側識別子	
Rooster側IPアドレス	
Rooster側ネットワーク	
Rooster側ネットマスク	
Rooster側識別子	test@test
メモ	

☑ セッションキープを行う。
☐ キープアライブを行う。
監視先IPアドレス1
監視先IPアドレス2
☐ バックアップ設定を使用する。
バックアップ設定

[設定] [キャンセル]

図 8-18　Rooster-LS の設定

8.7.4 Rooster-LS同士で、ダイナミックDNSを利用した場合

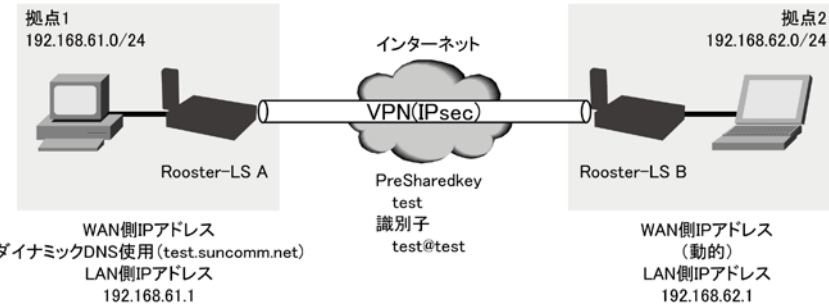



図 8-19 Rooster-LS A の WAN 側はダイナミック DNS を利用し、Rooster-LS B が動的の場合

- Rooster-LS A の設定例

VPNの詳細設定

項目	設定値
No.	1
プロトコル	IPsec
インターフェイス	モバイル通信端末
モード設定	アグレッシブモード
接続種別	レスポンダ
ハッシュアルゴリズム	SHA-1
暗号化アルゴリズム	AES256bit
PreSharedKey	test
IKE Life Time	3600 秒
IPsec Life Time	28800 秒
相手IPアドレス	0.0.0.0
相手ネットワーク	192.168.62.0
相手ネットマスク	255.255.255.0
相手側識別子	test@test
Rooster側IPアドレス	
Rooster側ネットワーク	
Rooster側ネットマスク	
Rooster側識別子	
メモ	

☐ セッションキープを行う。
☐ キープアライブを行う。
監視先IPアドレス1
監視先IPアドレス2
☐ バックアップ設定を使用する。
バックアップ設定

設定 キャンセル

図 8-20 Rooster-LS A の設定

- Rooster-LS B の設定例

VPNの詳細設定

項目	設定値
No.	1
プロトコル	IPsec
インターフェイス	モバイル通信端末
モード設定	アグレッシブモード
接続種別	イニシエータ
ハッシュアルゴリズム	SHA-1
暗号化アルゴリズム	AES256bit
PreSharedKey	test
IKE Life Time	3600 秒
IPsec Life Time	28800 秒
相手IPアドレス	test.suncomm.net
相手ネットワーク	192.168.61.0
相手ネットマスク	255.255.255.0
相手側識別子	
Rooster側IPアドレス	
Rooster側ネットワーク	
Rooster側ネットマスク	
Rooster側識別子	test@test
メモ	

☑ セッションキープを行う。
☐ キープアライブを行う。
監視先IPアドレス1
監視先IPアドレス2
☐ バックアップ設定を使用する。
バックアップ設定

設定 キャンセル

図 8-21 Rooster-LS B の設定

8.8 VRRP設定

VRRP について

VRRP（Virtual Router Redundancy Protocol）は、複数のルータが 1 つのグループに所属させ、通常はその中の 1 つのルータが通信を行ないますが、そのルータが障害を起こした際に同グループに属するルータが自動的に通信を受け継ぎ通信を行います。

Rooster-LS では、VRRP によるネットワークの冗長化を実現します。

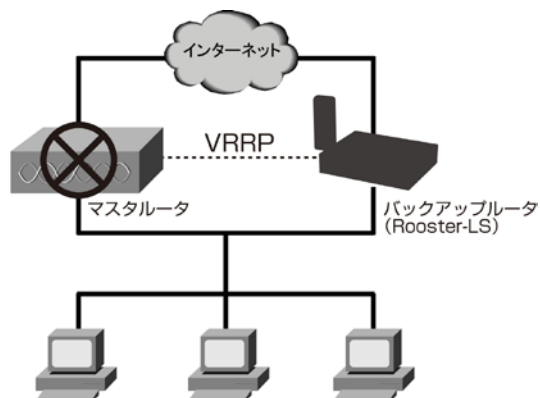



図 8-22 VRRP 概要図

1. 設定ツールのメニューから、[ネットワーク]－[VRRP]をクリックします。

ネットワーク

ネットワークの各設定を行います。

VRRP

VRRPの設定を行います。

☑VRRPを使用する。

仮想ルータID: 1

ホストの優先順位: 100

自動切戻し抑止時間: 5 秒

仮想ルータIPアドレス: 192.168.62.254

[設定]

図 8-23 Rooster-LS 側の設定

2. 「VRRP を使用する。」のチェックをオンにし、以下の設定を行います。

■ **仮想ルータ ID**

仮想ルータのグループID（VRID）を1から255の間で設定します。

メモ 同グループ ID 内に所属できる仮想ルータは最大 4 台までです。

■ **ホストの優先順位**

仮想ルータの優先度を1から254の間で設定します。仮想ルータIPアドレスと実IPアドレスを持つルータが稼動している場合は、そのルータは優先度255となります。
優先度値が最も大きいルータがマスタルータになります。また、マスタルータがダウンした場合、バックアップルータのうちで最も優先度値の高いルータがマスタルータになります

■ **自動切戻し抑止時間**

マスタルータに障害が発生してバックアップに切り替わったあと、障害が復旧した場合、優先度の高いバックアップのルータが自動的にマスタルータに切り替え処理を開始するまでの時間を設定します。
また、ここで設定した時間は、VRRP広告（生存確認）の送信間隔としても動作します。

■ **仮想ルータ IP アドレス**

仮想ルータへ仮想IPアドレスを設定します。仮想ルータIPアドレスと実IPアドレスを持つルータが稼動している場合は、そのルータは優先度255となります。

3. [設定] ボタンをクリックし、設定した内容を反映させます。

9. ログの参照方法

9.1 パケット通信ログ

> **注意** 工場出荷時状態では、Rooster-LS への負荷を軽減させるため、パケット通信ログは記録しない設定になっています。
>
> パケット通信ログを記録させる場合は、[ログ管理]の設定で「ログ管理を行う」のチェックをオンに設定してください。
>
> （設定方法は、☞ 7.9 ログ管理をご覧ください。）

9.1.1 パケット通過ログ

設定ツールのメニューから、[ログ]－[パケット通信ログ] －[通過ログ]をクリックします。
パケット通過ログ一覧のページが表示されます。

ログ

ログ表示の各設定を行います。

パケット通信ログ：通過ログ

通過パケットのログ一覧を表示します。

現在の時間は 2010/01/19 13:21:26 [再読込] [クリア]

No.	記録時間	通信タイプ	発信元IP	発信元ポート	送信先IP	送信先ポート	終了した理由
1	2010/01/19 13:21:14	UDP	192.168.62.50	53101	192.168.62.1	53	正常終了
2	2010/01/19 13:21:16	TCP	192.168.62.50	1757	[illegible]	80	正常終了
3	2010/01/19 13:21:16	UDP	192.168.62.50	53353	192.168.62.1	53	正常終了
4	2010/01/19 13:21:17	TCP	192.168.62.50	1758	[illegible]	80	正常終了
5	2010/01/19 13:21:17	UDP	192.168.62.50	52767	192.168.62.1	53	正常終了

図 9-1　　パケット通過ログ一覧画面

■ **No.**

ログの通し番号が表示されます。
番号が大きくなるほど、より新しいログとなります。

■ **記録時間**

時刻設定がされている場合、ログの発生した時刻が表示されます。

■ **通信タイプ**

IPパケットの種別（TCP、UDP、ICMPなど）が表示されます。

■ **発信元 IP**

通信の起点になる機器のIPアドレスが表示されます。

■ **発信元ポート**

通信の起点になる機器の使用ポート番号が表示されます。

■ **送信先 IP**

通信の宛先になる機器のIPアドレスが表示されます。

■ **送信先ポート**

通信の宛先になる機器の使用ポート番号が表示されます。

■ **終了した理由**

通信が終了した理由が表示されます。

正常終了

⇒正常に通信が行われた時に表示されます。

タイムアウト

⇒通信セッション確立後、通信が途中で終了、あるいは終了フラグを確認できなかった時に表示されます。

9.1.2 パケット遮断ログ

設定ツールのメニューから、[ログ]－[パケット通信ログ]－[遮断ログ]をクリックします。
パケット遮断ログ一覧のページが表示されます。

ログ

ログ表示の各設定を行います。

パケット通信ログ：遮断ログ

遮断パケットのログ一覧を表示します。

現在の時間は 2010/01/19 13:23:38 [再読込] [クリア]

No.	記録時間	通信タイプ	発信元IP	発信元ポート	送信先IP	送信先ポート
1	2010/01/19 13:22:26	TCP	[illegible]	6000	[illegible]	8080
2	2010/01/19 13:23:35	TCP	[illegible]	3966	[illegible]	8080
3	2010/01/19 13:23:38	TCP	[illegible]	3966	[illegible]	8080

図 9-2　　パケット遮断ログ一覧画面

■ **No.**

ログの通し番号が表示されます。
番号が大きくなるほど、より新しいログとなります。

■ **記録時間**

時刻設定がされている場合、ログの発生した時刻が表示されます。

■ **通信タイプ**

IPパケットの種別（TCP、UDP、ICMPなど）が表示されます。

■ **発信元 IP**

通信の起点になる機器のIPアドレスが表示されます。

■ **発信元ポート**

通信の起点になる機器の使用ポート番号が表示されます。

■ **送信先 IP**

通信の宛先になる機器のIPアドレスが表示されます。

■ **送信先ポート**

通信の宛先になる機器の使用ポート番号が表示されます。

9.2 回線ログ

9.2.1 モバイル通信端末ログ

設定ツールのメニューから、[ログ]－[回線ログ] －[モバイル通信端末ログ]をクリックします。
モバイル通信端末ログ一覧のページが表示されます。

ログ

ログ表示の各設定を行います。

回線ログ:モバイル通信端末ログ

モバイル通信端末の通信ログ一覧を表示します。

現在の時間は 2010/01/19 13:22:04 [再読込] [クリア]

No.	記録時間	ログ
1	2010/01/19 13:19:58	モバイル通信端末制御サービスを開始します
2	2010/01/19 13:20:39	モバイル通信端末をドコモFOMAとして認識しました
3	2010/01/19 13:20:39	--- モバイル通信端末を初期化します ----------
4	2010/01/19 13:20:42	ダイヤルを行ないます
5	2010/01/19 13:20:42	電話番号:*99***1#
6	2010/01/19 13:20:43	PPP接続開始
7	2010/01/19 13:20:49	PPP接続が確立しました

図 9-3　モバイル通信端末ログ一覧画面

■ **No**

ログの通し番号が表示されます。
番号が大きくなるほど、より新しいログとなります。

■ **記録時間**

時刻設定がされている場合、ログの発生した時刻が表示されます。

■ **ログ**

モバイル通信端末の動作状態が表示されます。
ダイヤルアップ接続、およびRAS着信接続が正常に行えない場合、以下のログ表示例をご確認いただき、該当する処置を行ってください。

受信：NO CARRIER
回線接続の確立に失敗しました（リザルトエラー）

⇒以下のいずれかの場合が考えられます。

1. ダイヤルアップ接続先の電話番号が間違っている。
   ⇒正しい電話番号を設定してください。
2. 電波状態が悪い。
   ⇒Rooster-LSを通信状態のよい場所に移動するか
   （できるだけ窓側あるいは高い場所）
   あるいは、しばらく時間を置いてやり直してみてください。

受信：DELAYED
回線接続の確立に失敗しました（リザルトエラー）

⇒3分間以内に3回以上、同一電話番号に電話を掛けようとすると、
モバイル通信端末に発信規制が掛かってしまいます。
一旦接続動作を解除して、しばらくお待ちいただいてからお掛け直しください。

PPP 接続でユーザ認証に失敗しました

⇒ダイヤルアップ接続のID、パスワードのいずれかに誤りがあります。
再度、ダイヤルアップ接続の設定の確認を行ってください。

電話番号認証に登録がありません
着信条件が合わない為、無視します

⇒RAS着信相手先リスト画面に登録されていない電話番号のため、
相手からの着信要求を無視しています。
RAS着信相手先リストに該当する番号を登録するか、着番認証のチェックをオフに設定してください。

9.2.2 VPNログ

設定ツールのメニューから、[ログ]－[回線ログ] －[VPNログ]をクリックします。
VPNログ一覧のページが表示されます。

No.	記録時間	ログ
20	2010/01/19 13:21:01	Using Linux 2.6 IPsec interface code on 2.6.23.17-rooster8 (experimental code)
21	2010/01/19 13:21:01	ike_alg_register_enc(): WARNING: enc alg=0 not found in constants.c:oakley_enc_names
22	2010/01/19 13:21:01	ike_alg_register_enc(): Activating <NULL>: Ok (ret=0)
23	2010/01/19 13:21:01	ike_alg_register_enc(): WARNING: enc alg=0 not found in constants.c:oakley_enc_names
24	2010/01/19 13:21:01	ike_alg_add(): ERROR: Algorithm already exists
25	2010/01/19 13:21:01	ike_alg_register_enc(): Activating <NULL>: FAILED (ret=-17)
26	2010/01/19 13:21:01	ike_alg_register_enc(): WARNING: enc alg=0 not found in constants.c:oakley_enc_names
27	2010/01/19 13:21:01	ike_alg_add(): ERROR: Algorithm already exists
28	2010/01/19 13:21:01	ike_alg_register_enc(): Activating <NULL>: FAILED (ret=-17)
29	2010/01/19 13:21:01	ike_alg_register_enc(): WARNING: enc alg=0 not found in constants.c:oakley_enc_names
30	2010/01/19 13:21:01	ike_alg_add(): ERROR: Algorithm already exists
31	2010/01/19 13:21:01	ike_alg_register_enc(): Activating <NULL>: FAILED (ret=-17)
32	2010/01/19 13:21:01	ike_alg_register_enc(): WARNING: enc alg=0 not found in constants.c:oakley_enc_names
33	2010/01/19 13:21:01	ike_alg_add(): ERROR: Algorithm already exists
34	2010/01/19 13:21:01	ike_alg_register_enc(): Activating <NULL>: FAILED (ret=-17)
35	2010/01/19 13:21:01	ike_alg_register_enc(): WARNING: enc alg=0 not found in constants.c:oakley_enc_names
36	2010/01/19 13:21:01	ike_alg_add(): ERROR: Algorithm already exists
37	2010/01/19 13:21:01	ike_alg_register_enc(): Activating <NULL>: FAILED (ret=-17)

図 9-4　　VPN ログ一覧画面

■ **No**

ログの通し番号が表示されます。
番号が大きくなるほど、より新しいログとなります。

■ **記録時間**

時刻設定がされている場合、ログの発生した時刻が表示されます。

■ **ログ**

VPNの動作状態が表示されます。
VPN接続が成功すると、「IPsecのNo.＊（＊はVPN設定リストのNo.）が接続完了しました」と表示されます。
接続できない場合、VPNの設定に誤りがないかどうかご確認ください。
VPNの設定につきましては、☞ 8.7 VPN設定をご覧ください。

9.3 サービスログ

9.3.1 アドレス解決ログ

設定ツールのメニューから、[ログ]－[サービスログ] －[アドレス解決ログ]をクリックします。
アドレス解決ログ一覧のページが表示されます。

ログ

ログ表示の各設定を行います。

サービスログ：アドレス解決ログ

アドレス解決ログ一覧を表示します。

現在の時間は 2008/01/02 02:16:47 再読込 クリア

No.	記録時間	ログ
1	2008/01/02 02:16:04	アドレス解決のプロセスが開始されました
2	2008/01/02 02:16:04	現在のIPを'suncomm.DDNS'へ登録します
3	2008/01/02 02:16:05	アドレス解決プロセスは正常終了しました

図 9-5　　アドレス解決ログ一覧画面

■ **No**

ログの通し番号が表示されます。
番号が大きくなるほど、より新しいログとなります。

■ **記録時間**

時刻設定がされている場合、ログの発生した時刻が表示されます。

■ **ログ**

アドレス解決機能の動作状態が表示されます。
「アドレス解決プロセスは異常終了しました」となる場合、以下のログ表示例をご確認いただき、該当する処置を行ってください。

● **アドレス解決をメール送信で行っている場合**

SMTP サーバ エラー : 535 Error: authentication failed

ユーザ認証SMTPのメールサーバで、[本体設定]-[メールアカウント設定]の、「アカウント」、「パスワード」のいずれかに誤りがある場合に表示されます。

SMTP サーバ エラー : 501 Syntax: MAIL FROM:

ユーザ認証SMTPのメールサーバで、[各種サービス]-[アドレス解決]の、「送信元メールアドレス」の設定がされていないか、書式に誤りがある場合に表示されます。

SMTP サーバ エラー : 572 Relay not authorized

POP before SMTPのメールサーバで、[本体設定]-[メールアカウント設定]の「サービスの種類」に「ユーザ認証SMTP」の設定を行った場合に表示されます。

● **アドレス解決を suncomm.DDNS で行っている場合**

suncomm.DDNS サーバ エラー

suncomm.DDNSの設定に誤りがある場合に表示されます。

9.3.2 DHCPログ

設定ツールのメニューから、[ログ]－[サービスログ]－[DHCPログ]をクリックします。DHCPログ一覧のページが表示されます。

ログ

ログ表示の各設定を行います。

サービスログ:DHCPログ

DHCPログ一覧を表示します。

現在の時間は 2010/01/19 13:25:47 再読込 クリア

No.	記録時間	ログ
1	2010/01/19 13:21:02	[illegible]に192.168.62.50を割り当てました

図 9-6 DHCP ログ一覧画面

■ **No**

ログの通し番号が表示されます。
番号が大きくなるほど、より新しいログとなります。

■ **記録時間**

時刻設定がされている場合、ログの発生した時刻が表示されます。

■ **ログ**

DHCP機能の動作状態が表示されます。

9.3.3 WANハートビートログ

設定ツールのメニューから、[ログ]－[サービスログ]－[WAN]ハートビートログをクリックします。WANハートビートログ一覧のページが表示されます。

ログ

ログ表示の各設定を行います。

サービスログ:WANハートビートログ

WANハートビートログ一覧を表示します。

現在の時間は 2010/01/19 13:31:38 再読込 クリア

No.	記録時間	ログ
1	2010/01/19 13:29:35	WANハートビートのプロセスが開始されました
2	2010/01/19 13:29:35	成功しました
3	2010/01/19 13:30:36	成功しました
4	2010/01/19 13:31:37	成功しました

図 9-7 WAN ハートビートログ一覧画面

■ **No**

ログの通し番号が表示されます。
番号が大きくなるほど、より新しいログとなります。

■ **記録時間**

時刻設定がされている場合、ログの発生した時刻が表示されます。

■ **ログ**

WANハートビート機能の動作状態が表示されます。

9.3.4 PPPログ

> **注意** 工場出荷時状態では、Rooster-LS への負荷を軽減させるため、PPP ログは記録しない設定になっています。
>
> PPP ログを記録させる場合は、[ログ管理]の設定で「PPP ログを有効にする」のチェックをオンに設定してください。
>
> （設定方法は、☞ 7.9 ログ管理をご覧ください。）

設定ツールのメニューから、[ログ]－[サービスログ] －[PPPログ]をクリックします。
PPPログ一覧のページが表示されます。

ログ

ログ表示の各設定を行います。

サービスログ：PPPログ

PPPログ一覧を表示します。

現在の時間は 2010/01/19 13:26:54 [再読込] [クリア]

No.	記録時間	ログ
1	2010/01/19 13:20:43	pppd options in effect:
2	2010/01/19 13:20:43	debug # (from /etc/ppp/peers/ppp_client)
3	2010/01/19 13:20:43	kdebug 0 # (from command line)
4	2010/01/19 13:20:43	logfile sclog # (from /etc/ppp/peers/ppp_client)
5	2010/01/19 13:20:43	unit 1 # (from command line)
6	2010/01/19 13:20:43	dump # (from /etc/ppp/peers/ppp_client)
7	2010/01/19 13:20:43	user test # (from command line)
8	2010/01/19 13:20:43	/dev/ttySC0 # (from command line)
9	2010/01/19 13:20:43	115200 # (from command line)
10	2010/01/19 13:20:43	lock # (from command line)
11	2010/01/19 13:20:43	connect /usr/local/sbin/ppp-on-dialer # (from command line)
12	2010/01/19 13:20:43	crtscts # (from command line)
13	2010/01/19 13:20:43	modem # (from command line)
14	2010/01/19 13:20:43	noipdefault # (from command line)
15	2010/01/19 13:20:43	defaultroute # (from command line)
16	2010/01/19 13:20:43	usepeerdns # (from command line)
17	2010/01/19 13:20:43	netmask 255.255.255.0 # (from command line)
18	2010/01/19 13:20:43	: # (from command line)
19	2010/01/19 13:20:43	lcp_open. custom_termreq 0

図 9-8　　PPP ログ一覧画面

■ **No**

ログの通し番号が表示されます。
番号が大きくなるほど、より新しいログとなります。

■ **記録時間**

時刻設定がされている場合、ログの発生した時刻が表示されます。

■ **ログ**

PPPの動作状態が表示されます。

9.4 その他ログ

9.4.1 システムログ

設定ツールのメニューから、[ログ]－[その他ログ] －[システムログ]をクリックします。
システムログ一覧のページが表示されます。

ログ

ログ表示の各設定を行います。

その他のログ：システムログ

システムログ一覧を表示します。

現在の時間は 2010/01/19 13:31:16 [再読込] [クリア]

No.	記録時間	ログ
1	2010/01/19 13:28:28	ログシステムの開始
2	2010/01/19 13:28:28	ソフトウェアによる自動電源ON/OFF機能を開始します
3	2010/01/19 13:28:28	ソフトウェアによる自動電源ON/OFF機能を毎日の03:00に設定しました

図 9-9　　システムログ一覧画面

■ **No**

ログの通し番号が表示されます。
番号が大きくなるほど、より新しいログとなります。

■ **記録時間**

時刻設定がされている場合、ログの発生した時刻が表示されます。

■ **ログ**

Rooster-LSのシステムに関するログが表示されます。

製品仕様

項目		仕様
製品名		Rooster-LS(ルースター エルエス)
型名		SC-RS510LS
JAN コード		4907940130063
ルーティング方式		スタティックルーティング ダイナミックルーティング
インターフェイス		MDI/MDI-X 自動判別
ハードウェア構成	LAN ポート	100BASE-T/10BASE-T ×2 ポート
	USB	USB2.0/HOST 機能対応×2 ポート
	LED	11 個
	CPU	Marvell Orion Processor(400MHz)
	メインメモリ	128MB(DDR2)
	フラッシュメモリ	16MB
リセットスイッチ		1 個
電源仕様		AC アダプタ
	定格入力	AC100V (50/60Hz)
	定格出力	DC1.0A (DC12V)
	最大消費電力	11W
環境条件	温度	5～40℃
	湿度	25～85%(結露なきこと)
	耐ノイズ性 ※1 AC ラインノイズ DC ラインノイズ	 ±2000V パルス幅 100ns/1000ns ±2000V パルス幅 100ns/1000ns ノイズシミュレータによる
	耐静電気性 ※1 直接放電 気中放電	 ±10KV LAN 端子金属部 ±10KV LAN 端子金属部
重量		300g(本体のみ)
外形寸法		128(H)×104(D)×28(W) 単位 mm (付属物/ケーブル/突起物は含まず)
サポートプロトコル	Ethernet	CSMA/CD
	ルーティング	IP のみ
	認証	PAP、CHAP、MS-CHAPv2
	暗号化	MPPE128bit
	WAN プロトコル	PPP
	管理プロトコル	SNMPv1
	ルーティングプロトコル	RIP v1、v2
WAN 接続方式		numbered、unnumbered、ビジネス mopera
DHCP		・サーバ機能(LAN 側最大 253 クライアント) ・リレー機能
アドレス変換		NAT/IP マスカレード
VPN パススルー		IPsec/PPTP パススルー

項目		仕様
サーバー公開		バーチャルサーバ(最大 16 件設定可) DMZ ホスト(1 件設定可)
スタティックルーティングテーブル		最大 32 件登録可能
アップデート		・WWW ブラウザによるアップデート
WakeOn 着信	メッセージ認証登録	メッセージ登録(128 文字)/1 件
	着信番号登録	CLID/16 件
アドレス解決	アドレス登録	1 件
	メッセージ登録	1 件
	プロトコル	SMTP、POP
	ダイナミック DNS	suncomm.DDNS
	更新時間設定	可能 (5 分～)
WAN ハートビート	相手先	WAN ゲートウェイ、任意のアドレス設定
	更新時間設定	可能 (1 分～)
無通信監視タイマー		設定可能
電源制御		・ハードウェアおよびソフトウェア ・モバイル通信端末 ※本体電源 OFF から 10 秒±5 秒で電源 ON
ハードウェアウォッチドッグ 信号受信タイミング 発動条件		 常時監視(1 秒毎) 信号不受信から約 1 分 30 秒後
ダイアルアップ自動発信条件		・LAN 側からのパケット送出 ・ダイヤルアップ/セッションキープ ・ダイヤルアップ/キープアライブ ・IPsec/セッションキープ ・IPsec/キープアライブ ・WAN ハートビート ・NTP
ダイヤルアップ手動発信/切断		可能
ダイヤルアップ先設定		1 件
ダイヤルアップセッションキープ		可能
リモートアクセス	プロトコル	PIAFS2.2/2.1/2.0/1.0/FOMA64K (モバイル通信端末に依存)
	認証方式	PAP、CHAP,MS-CHSPv2,CLID×50 件
	暗号化	MPPE128bit
回線冗長化		VRRP(バーチャルルータ設定 4 件)
WAN 側 IP アドレス固定		可能
対向通信		可能
ビジネス mopera アクセスプレミアム		発信及び IP 着信可能、Radius 認証対応
ビジネス mopera アクセスプロ		発信可能
MPPE 暗号化		128bit
Unnumbered 接続		可能
モバイル端末情報		自局電話番号、電界強度、位置情報、APN、MAC アドレス※端末によっては表示されない機種もございます。

モバイル端末設定		APN16 件 PIN コード解除
VPN 機能	暗号化	IPsec(VPN 機能) AES256bit、3DES
	アルゴリズム	IKE (メインモード、アグレッシブモード)
	接続可能数	最大 16 件
	接続要求	イニシエータ、レスポンダ
	セッションキープ設定	可能
	キープアライブ設定	可能
	バックアップ設定	別 VPN 装置への接続設定可能 (1 セッションにつき 1 件)
	LifeTime 設定	可能
QoS 機能		優先制御、帯域制御 IP アドレス、ポート番号 最大 8 件登録可能
ロギング		・WWW ブラウザによる各種ログ表示 ・Telnet による各種ログ表示 ・Syslog での出力 ・USB メモリへの出力
ログの内容		・パケット通過ログ/遮断ログ ・モバイル通信端末ログ ・アドレス解決ログ ・DHCP ログ ・WAN ハートビートログ ・VPN ログ ・PPP ログ ・システムログ
設定情報管理		・WWW ブラウザによるファイル保存、読み込み ・Telnet 上でのコマンドによる読み込み、書き込み
FORWARD フィルタリング		最大 32 件登録可能 以下の各パラメータによるフィルタリング ・インターフェイス ・方向 ・動作(許可または遮断) ・プロトコル ・相手 IP アドレス ・相手ポート
INPUT フィルタリング		最大 64 件登録可能 以下の各パラメータによるフィルタリング ・動作(許可または遮断) ・プロトコル ・相手 IP アドレス ・ネットマスク ・相手ポート
設定方法		WWW ブラウザ、TELNET による設定
インターネット経由のリモートセットアップ		可能

時刻管理	設定方法	NTP サーバ設定/手動設定
	更新時間設定	可能
保証		1 年間
付属品 ※2		・スタートアップマニュアル(保証書付)---1 枚 ・AC アダプタ---1 個 ・電源抜け防止クランプ---1 個 ・ゴム足---4 個

※1 ノイズを印加し続けた際の動作を保証するものではございません。
※2 付属品にLANケーブルは含まれません。設定で使用するLANケーブルにつきましては
ご利用の接続機器の速度に合わせてご用意ください。

サポートのご案内

- **最新情報の入手**

Rooster-LSに関する最新情報は、弊社ホームページから入手することができます。また、バージョンアップ情報につきましても公開しております。

■ **製品紹介ページ**

http://www.sun-denshi.co.jp/sc/ls/

- **ご質問・お問い合わせ**

Rooster-LSに関するご質問やお問い合わせは、下記へご連絡願います。

ユーザー　サポートセンター

- 電話　0587-55-0161
- FAX　0587-55-0815
- メール　support-suncomm@sun-denshi.co.jp
- 受付時間　月曜～金曜　10:00～16:00（12:00～13:00 を除く）
  祝日、弊社休日を除く

SC-RS510LS
取扱説明書　Ver.7.00

2014 年 10 月発行

サン電子株式会社

〒483-8555　愛知県江南市古知野町朝日 250

(141015)